4/2019

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

42. Jahrgang
ISSN 0137-7767
12,00 Euro

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Minderjährigen(daten)schutz

■ Vor und nach der Geburt – aus Sicht des Datenschutzes ■ Datenschutz im Kindergarten ■ Praktische Sensibilisierung an Schulen ■ Eltern – gesetzliche Vertreter oder Dritte? ■ Digitale Sorge, Mediennutzung und Datenschutz ■ Online-Spiele: Was geschieht mit den Daten ■ Die Vernetzung von Patientendaten im Gesundheitssystem ■ Nachrichten ■ Rechtsprechung ■

Inhalt

Termine



Foto: Pixabay..com

Samstag, 25. Januar 2020
DVD-Vorstandssitzung
Bonn

Montag, 27. Januar 2020
PinG-Jahrestagung Datenschutz 2020
Berlin

Montag, 27. Januar 2020
Europäische Akademie Berlin „Was bleibt, was muss sich ändern?" Evaluation der Datenschutz-Grundverordnung

Dienstag, 28. Januar 2020
Europäischer Datenschutztag 2020

Samstag, 01. Februar 2020
Redaktionsschluss DANA 1/2020
„Gesundheits-(Daten)schutz"

Dienstag, 11. Februar 2020
Safer Internet Day 2020 in Europa

Donnerstag, 30. April 2020
Big Brother Awards
Stadttheater Bielefeld

Freitag, 01. Mai 2020
Redaktionsschluss DANA 2/2020
„e-Payment"

DANA
Datenschutz Nachrichten
ISSN 0137-7767
42. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Heinz Alenfelder, Susanne Holzgraefe
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, Shutterstock, ClipDealer

Editorial

Babyphone, Alexa und Co., Überwachungskameras im öffentlichen Nahverkehr, an öffentlichen Plätzen, in Schulen und Mietshaus-Treppenhäusern sowie die Vielzahl weiterer Alltagshelfer sorgen heute schon dafür, dass unsere Jüngsten schon sehr früh an Überwachung gewöhnt werden und die Entwicklung des Gefühls für Privatheit immer schwieriger wird. Hinzu kommt der Stolz auf die Jüngsten vieler Eltern, die viele Momente der Kinder festhalten und mit anderen teilen möchten.

Gerade Kinder und Jugendliche sind der ständigen Gefahr der Verletzung ihrer Privatheit ausgesetzt. Vieles passiert unbedacht. Es ist wichtig, dass sowohl Kinder und Jugendliche als auch die Eltern und Erziehungsberechtigten sowie Betreuende und andere Menschen aus dem Umfeld der Kinder und Jugendlichen für den Schutz der Privatheit und die Gefahren, die die Weitergabe und Veröffentlichung von persönlichen Informationen mit sich bringen, sensibilisiert werden.

Fotos, die früher in der kommunalen Tageszeitung veröffentlicht wurden, wurden kaum außerhalb der Kommune wahr genommen. Durch die digitale Präsenz der Tageszeitung sind die Fotos heute weltweit abrufbar. Auch mussten früher mühevoll die Zeitungsarchive nach älteren Artikeln durchsucht werden, wo hingegen heute ältere Artikel schnell und einfach online verfügbar sind. Während bei der älteren Generation Fotos, Filme und Artikel aus Kindertagen in dunklen Archiven und Schubladen verschwunden und in Vergessenheit geraten sind, sind sie bei der jüngeren Generation jederzeit einfach und schnell weltweit verfügbar.

In der vorliegenden DANA-Ausgabe widmen sich die Autoren dem Thema Datenschutz bei Kindern und Jugendlichen und nehmen hier verschiedene Aspekte aus deren Alltagsleben genauer unter die Lupe.

Darüber hinaus berichtet Anne Riechert aus gegebenem Anlass über die Vernetzung von Patientendaten im Gesundheitswesen.

Am Ende des Magazins sind wie üblich die Datenschutz- und Techniknachrichten, aktuelle Rechtsprechungen und Buchbesprechungen zu finden.

Die DANA-Ausgabe zeigt, dass es noch viel zu tun gibt. Es wird wieder viel Spannendes für die winterliche Lektüre geboten. Viel Kurzweile und Erkenntnisgewinn wünschen wir dabei.

Susanne Holzgraefe

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied in der DVD,
alenfelder@datenschutzverein.de, Köln

Dr. Susanne Holzgraefe
Vorstandsmitglied in der DVD, holzgraefe@datenschutzverein.de

Prof. Dr. Anne Riechert
Wissenschaftliche Leiterin der Stiftung Datenschutz
a.riechert@stiftungdatenschutz.org

Klaus-Jürgen Roth
dvd@datenschutzverein.de

Dipl.-Inf. Michael Schlegel
USU GmbH, Möglingen

Prof. Dr. Tobias Straub
Duale Hochschule Baden-Württemberg, Stuttgart
tobias.straub@dhbw-stuttgart.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Thilo Weichert

Vor und nach der Geburt – aus Sicht des Datenschutzes[1]

Eine Geburt ist ein höchst körperlicher, analoger Prozess. Doch sind mit ihr viele informationelle digitale Aktivitäten verbunden. Da Hebammen, die Eltern sowie weitere Beteiligte in dieser Situation etwas anderes als Datenschutz im Kopf haben, dieser aber angesichts der Sensibilität der Vorgänge wie auch der dabei entstehenden Daten von hoher Bedeutung ist, ist es sinnvoll, sich hiermit näher zu befassen.

Geburten werden gerne als Beispiel dafür herangezogen, dass der Auswertung von digitalen Daten nur begrenzt getraut werden kann: In den 90er Jahren des letzten Jahrhunderts wurde festgestellt, dass zwischen den Daten über das Storchvorkommen und über Geburten eine hohe statistische Korrelation bestand. So unsinnig es wäre, hieraus den Schluss zu ziehen, dass Störche die Kinder bringen, so wichtig ist es generell darauf hinzuweisen, dass Analyseergebnisse aus Big Data nicht zwingend auf Kausalitäten, ja nicht einmal auf gemeinsame Hintergründe hinweisen, sondern zufällig sein können.[2]

Big Data kann auch valide Erkenntnisse liefern, wie ein weiteres einschlägiges, oft kommuniziertes Beispiel aus dem Jahr 2012 zeigt: Die US-Supermarkt-Kette Target analysierte das Einkaufsverhalten seiner Kundinnen auf Besonderheiten bei Schwangerschaften hin, um frühzeitig den schwangeren Frauen passgenaue Verkaufsangebote zu unterbreiten. Darüber erfuhr ein Vater in Minnesota, dass seine minderjährige Tochter ein Kind erwartete.[3]

Big Data dient oft legitimeren Zwecken als der Werbung: Es geht darum, wichtige wissenschaftliche Erkenntnisse zu erlangen, etwa in der medizinischen Forschung. Es ermöglicht einen effektiveren Ressourceneinsatz etwa in der Krankenhausplanung oder bei der Medikamentenversorgung. Big Data kann dabei helfen, effektiver und wirtschaftlicher Aufgaben zu erfüllen. Bei der Qualitätssicherung medizinischer Versorgung kann Big Data eine wichtige Hilfe sein.[4] Dies gilt auch für die Prozesse vor und nach der Geburt.

Informationsprozesse bei der Geburtshilfe

Informationstechnik ist in der Geburtshilfe heute ein oft unersetzliches Hilfsmittel. Sie erleichtert es den Hebammen und den Entbindungspflegern bzw. den in diesem Bereich tätigen Einrichtungen, ihren administrativen Aufgaben nachzukommen. Gemäß § 301a SGB V sind Hebammen für Abrechnungszwecke verpflichtet, den Kassen gegenüber elektronisch Angaben über die von ihnen betreuten Frauen zu machen einschließlich der erbrachten Leistungen, Zeit und Dauer, zurückgelegten Wege und Auslagen. Diesem Zweck dienen Software-Angebote sowohl für den ambulanten als auch für den stationären Bereich. Integrierbar sind Lesegeräte für die elektronischen Gesundheitskarte (§ 291a SGB V).

Diese Services beschränken sich nicht auf die Abrechnung mit Kassen, Privaten und Sonstigen; weitere Nutzungsmöglichkeiten sind z. B. die Adress- und Terminverwaltung, ein Kalender bis hin zu Werkzeugen zum Qualitätsmanagement. Die Erfassung erfolgt zumeist nicht nur auf stationären Rechnern, sondern ist auch mit mobilen Geräten möglich. Angeboten werden zumeist zudem die Wartung der Hard- und Software, automatisierte Plausibilitätsprüfungen, die Datensicherung oder eine Datenspeicherung in der „Cloud", also bei einem Dienstleister. Üblich sind Schnittstellen oder integrierte Dienste z. B. für die Buchhaltung bis hin zur Selektion steuerrelevanter Daten oder die E-Mail-Kommunikation.[5] Angebote für den stationären medizinischen Bereich sind integriert in die umfassenden Krankenhausinformationssysteme.[6] In Krankenhäusern wie im ambulanten Bereich kommen zunehmend neben oder statt der Dokumentation auf Karteikarten und Krankenakten digitalisierte Patientenakten zur Anwendung, die über Netze weiteren Dienstleistern zum Abruf zur Verfügung gestellt werden können. Hierüber wird teilweise eine sektorenübergreifende Kommunikation zwischen ambulantem und stationärem Bereich realisiert. Modelle, bei denen selbst die Betroffenen über das Internet Zugriff auf ihre Akten nehmen können, sind in der Erprobung oder gar schon im Wirkbetrieb.

Regulativer Rahmen

Arbeitsteilung und Komplexität unseres Gesundheitssystems machen im Bereich der Geburtshilfe oft den Austausch von Daten notwendig. Hierzu gibt es Regeln. Diese entsprechen weitgehend den für Ärzte geltenden Normen und finden sich insbesondere im Medizin- und im Datenschutzrecht. Im Hinblick auf die Geburt gibt es weitere Vorgaben im Melde- oder im Sozialrecht.

Für den Datenschutz gelten seit Mai 2018 die Regeln der europäischen Datenschutz-Grundverordnung (DSGVO). Diese legt sowohl materielle als auch technische und organisatorische Anforderungen fest. Bei den materiellen Anforderungen kann unterschieden werden zwischen der Zulässigkeit der konkreten Verarbeitung und der Umsetzung der Betroffenenrechte.

Das Datenschutzrecht gilt nur für natürliche Personen, also hier für die Neugeborenen. Tatsächlich kann eine informationelle Fremdbestimmung schon zuvor, vom Zeitpunkt der Befruchtung einer Eizelle an, etwa über Genomanalyse, erfolgen. Entscheidungen vor der Geburt können die spätere Selbstbestimmung beeinträchtigen. Insofern ist dem Recht auf informationelle Selbstbestimmung eine vorgeburtliche Vorwirkung beizumessen.[7]

Der mit den Patientinnen abgeschlossene Geburtshilfe-Vertrag ist die Grundlage der Datenverarbeitung. Es handelt sich dabei um einen Behandlungsvertrag im Sinne von §§ 630a ff. des Bürger-

lichen Gesetzbuchs (BGB). Soll über diesen Rahmen hinausgegangen werden, z. B. durch Nutzung der Daten für Werbezwecke oder durch Einschaltung von Dritten bei der Leistungserbringung, so ist in jedem Fall eine spezifische Information, möglicherweise sogar eine ausdrückliche Einwilligung erforderlich. Bei Angaben zur Geburtshilfe handelt es sich um sensitive Gesundheitsdaten, die gemäß Art. 9 DSGVO unter einem verstärkten Schutz stehen. Nur Daten, die zur Erbringung der Dienste nötig sind, dürfen erfasst werden und sie dürfen grds. nicht für weitere Zwecke genutzt werden. Eine solche Zweckänderung kann durch Gesetz erlaubt sein, so wie dies im SGB V zum Zweck der Abrechnung mit den Krankenkassen vorgesehen ist. Bei Einwilligungen zur Datenweitergabe muss ein expliziter Hinweis erfolgen, dass Gesundheitsdaten übermittelt werden.

Vertrauensschutz

Hebammen unterliegen als „Angehörige eines Heilberufs" ebenso wie z. B. ÄrztInnen dem Patientengeheimnis, also einer beruflichen Schweigepflicht. Dieses Patientengeheimnis ist in § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) sowie in den Hebammenregelungen der Bundesländer ausdrücklich normiert. Sollen Daten aus der Berufsausübung weitergegeben werden, so muss in der Einwilligung zugleich eine Entbindung von der Schweigepflicht liegen. Lange Zeit bestand Rechtsunsicherheit, ob die beruflich erlangten Daten im Rahmen der Administration der informationstechnischen Programme und der Systemwartung den damit betrauten Technikern zur Kenntnis gelangen dürfen. Durch eine Gesetzesänderung ist insofern 2017 Rechtssicherheit hergestellt worden: Soweit erforderlich, dürfen diese, ebenso wie sonstige berufliche Gehilfen (Beschäftigte), die Daten der Gebärenden sowie sonstiger Personen aus deren Umfeld als „mitwirkende Personen" zur Kenntnis nehmen. Zugleich werden sie aber selbst gesetzlich zur Verschwiegenheit verpflichtet (§ 203 Abs. 3, 4 StGB).

Bei der Geburtshilfe ist eine zentrale Voraussetzung für ein ungestörtes Vertrauensverhältnis zwischen Hebamme, weiteren Helfenden einerseits und der (werdenden) Mutter und ihrem persönlichen Umfeld andererseits die Beachtung der Schweigepflicht. Schwangere und junge Mütter sind in einer körperlichen und psychologischen Ausnahmesituation und deshalb besonders verletzbar. Verletzungen, auch wenn diese über Datenverarbeitungen bzw. über digitale Prozesse erfolgen, sind unbedingt zu vermeiden.

Zur Beschränkung der Angriffsmöglichkeiten auf die Vertraulichkeit muss elektronische Kommunikation grds. verschlüsselt erfolgen. Hierfür bietet sich im Bereich der E-Mail-Kommunikation die Verwendung von „Pretty Good Privacy" (PGP) an. Die Speicherung von Daten – sei es in der Cloud oder auf dem eigenen Rechner – sollte mit einem Zugangsschutz und einer Verschlüsselung abgesichert werden. Die technischen Möglichkeiten hierfür sind von den Software- und Dienste-Anbietern bereitzustellen. Um dies nachzuweisen, berufen sich einige Anbieter auf externe Zertifizierungen. Dabei ist Vorsicht angesagt: Der Wert von Zertifikaten ist unterschiedlich und oft gering, auch wenn diese z. B. von TÜV-Unternehmen stammen. Staatlich anerkannt sind bisher nur die Zertifikate des Bundesamtes für die Sicherheit in der Informationstechnik (BSI). Künftig soll es auch eine unabhängige und transparente Datenschutz-Zertifizierung gemäß der DSGVO geben (Art. 42, 43 DSGVO).

Die Schweigepflicht hat Grenzen. Stellen Hebammen, ÄrztInnen oder sonstiges medizinisches Personal fest, dass für das neugeborene Kind eine konkrete Gefahr für Leib und Leben besteht, so sind sie berechtigt und verpflichtet, das Jugendamt zu informieren.[8] Dort können dann gemäß § 8a SGB VIII die weiteren erforderlichen Maßnahmen ergriffen werden. Auch bei einer konkreten Gefährdung für die Leibesfrucht oder die Mutter können von den medizinischen Hilfspersonen die (informationellen) Maßnahmen ergriffen werden, die zur Abwehr dieser Gefahr erforderlich sind.

Kein Problem mit der Vertraulichkeit bzw. dem Datenschutz besteht, wenn Daten vor ihrer Weitergabe wirksam anonymisiert werden. Wann davon gesprochen werden kann, ist aber höchst streitig. So ist es z. B. bei Softwareanbietern im ambulanten Arztbereich weit verbreitet, dass Kostenabschläge für die Praxen eingeräumt werden, wenn pseudonymisierte Daten über Behandlung und Medikation aus den Systemen abgezogen werden dürfen. Diese Daten werden dann an medizinische Informationsdienstleister, an die Pharmaindustrie oder an Forschungseinrichtungen weiterverkauft. Dies ist fragwürdig, da von den weitergegebenen Einzeldatensätzen mit etwas Zusatzwissen wieder auf einzelne Personen zurückgeschlossen werden kann.

Dokumentation und Kommunikation

Ein zentraler Aspekt der Datenverarbeitung bei der Geburtshilfe ist die Dokumentationspflicht der Hebamme bzw. der tätigen Einrichtung. Ebenso wie im ärztlichen Bereich sind die Betreuungsdaten über 10 Jahre hinweg zwingend aufzubewahren, um im Nachhinein die Versorgung der Mutter vollständig nachvollziehen zu können und im Konfliktfall als Beweismittel zur Verfügung zu stehen (§ 630f BGB). Falsch erfasste Daten dürfen nicht gelöscht, sondern müssen durch eine ergänzende Korrektur bereinigt werden. Mit dieser medizinrechtlichen Dokumentationspflicht korrespondiert der datenschutzrechtliche Grundsatz der Datenrichtigkeit (Art. 5 Abs. 1 lit. d DSGVO).

Bei Hebammen besteht oft Unsicherheit, ob über die 10 Jahre hinausgehend eine Dokumentation erfolgen darf oder gar muss. Tatsächlich besteht nach dem Zivilrecht in besonderen Ausnahmefällen die Möglichkeit, dass auch noch danach, bis zu 30 Jahre später, Schadenersatzforderungen gestellt werden (§ 199 Abs. 2 BGB). Die normale Verjährungsfrist beträgt nach § 195 BGB jedoch 3 Jahre. Die Reklamation von Behandlungsfehlern nach mehr als 10 Jahren dürfte die absolute Ausnahme darstellen. Da nach 10 Jahren die Dokumentation vernichtet werden darf, kann einer Hebamme wegen gelöschter Daten danach kein Vorwurf gemacht werden.

Die Dokumentation der sensitiven Daten muss vertraulich und sicher erfolgen (Art. 32 DSGVO).

Von der Datenverarbeitung Betroffene, also im Bereich der Geburtshilfe vor-

rangig die Mütter, haben Rechte. Hierzu gehört ein Anspruch auf umfassende Information über die erfolgenden Verarbeitungsprozesse (Art. 12, 13 DSGVO, vgl. § 630e BGB). Diese Unterrichtung muss ungefragt schon bei der Datenerhebung erfolgen. Auf Anfrage hin haben die Betroffenen zudem einen umfassenden Anspruch auf Datenauskunft, also auf Information über alles, was zu ihrer Person gespeichert ist, für welche Zwecke und an wen Daten weitergegeben wurden bzw. werden (Art. 15 DSGVO, § 630g BGB).

Eigentlich hätte schon im Jahr 2006 die elektronische Gesundheitskarte (eGK) eingeführt sein sollen, mit der die Kommunikation medizinischer Dienstleister über eine Telematik-Infrastruktur (TI) ermöglicht wird. Damit soll die Identifizierung der Patientinnen bei den Leistungserbringern sowie der Datenaustausch zwischen diesen über gesundheitsrelevante Umstände erleichtert werden. Konflikte zwischen den Organisationen im TI-Organisationsverbund „Gematik" sowie leider oft wenig qualifizierte Kritik insbesondere aus der Ärzteschaft führten dazu, dass auch im Jahr 2019 noch keine umfassende Einführung erfolgt ist und wichtige Funktionen fehlen. Bei der Kritik an der eGK wurde oft mit dem Datenschutz argumentiert, obwohl sowohl die technische Gestaltung der TI als auch die erlassenen gesetzlichen Regelungen (§ 291a SGB V) einen optimalen Vertraulichkeitsschutz gewährleisten sollen. Ob dies aber auch in die Realität umgesetzt wird, bleibt unklar. Dies bedeutet, dass beim weiteren Aufbau der TI und der Einbeziehung der Hebammen darauf geachtet werden muss, dass hierüber Datenschutz und Datensicherheit gewahrt bleiben.

Aus informationeller Sicht völlig neue Perspektiven auf die Geburt eröffnen sich mit der Entwicklung der Genomanalyse: Sie ermöglicht im Rahmen der Präimplantationsdiagnostik die Auswahl genetisch gesunder Spermien und Eizellen, eröffnet grds. aber auch die Möglichkeiten jenseits der Gesundheit die genetische Selektion nach gewünschten Kindes-Eigenschaften.[9] Während der Schwangerschaft sind für medizinische Untersuchungen nicht mehr die nicht ganz ungefährlichen Fruchtwasseruntersuchungen nötig, um bestimmte Risiken oder Eigenschaften auszuschließen. Über die Untersuchung des Mutterblutes eröffnen sich weitgehende pränataldiagnostische Perspektiven. Diese können in spezifische therapeutische Maßnahmen einfließen, aber auch in eine Entscheidung über einen Schwangerschaftsabbruch. Am 19.09.2019 beschloss der Gemeinsame Bundesausschuss, dass unter engen Voraussetzungen derartige Untersuchungen auf Down-Syndrom von den gesetzlichen Krankenkassen bezahlt werden.[10]

Geburt als administrativer Vorgang

Schwangerschaft und Geburt führen zu einem neuen kleinen Erdenmenschen. Damit verbunden sind einige – heute weitgehend digitalisierte – Verwaltungsvorgänge. Ohne Identifizierung und Registrierung ist ein Kind für die Verwaltung nicht existent. Schon mit der Schwangerschaft erhält die werdende Mutter einen Mutterpass. Die zuständige Krankenkasse wird über den voraussichtlichen Geburtstermin informiert, damit Mutterschaftsgeld und evtl. eine Haushaltshilfe gewährt werden kann. Der Arbeitgeber wird informiert, dem während der Schwangerschaft Schutzpflichten auferlegt sind. Er darf auf Anfrage hin den Betriebsrat informieren.[11] Erwerbslose Schwangere können die Agentur die Agentur für Arbeit, das Jobcenter oder das Sozialamt informieren, um eine Erhöhung des Leistungssatzes zu erreichen.

Eine Spezialität ist die anonyme bzw. „vertrauliche" Geburt, die seit Anfang 2014 gesetzlich zugelassen ist.[12] Deren Ziel ist es, Müttern, die sich in einer Notlage befinden, die Möglichkeit zu geben, ein gesundes Kind zu gebären, ohne dass dadurch die Notlage verschärft wird, also um sowohl Kind wie Mutter zu schützen. Der Mutter wird gesetzlich für 16 Jahre Anonymität zugesichert. Anonyme Geburten oder die anonyme Abgabe von Neugeborenen (über die sog. Babyklappe) führen dazu, dass die informationelle Verbindung zwischen Mutter und Kind langfristig gekappt wird. Dessen ungeachtet erkennt unser Rechtssystem an, dass jeder Mensch die Möglichkeit haben muss, seine biologischen Wurzeln, also Mutter und Vater, zu kennen.[13]

Die Geburt selbst muss binnen einer Woche dem Standesamt am Geburtsort gemeldet werden. Diese Aufgabe übernimmt die Einrichtung, die Geburtshilfe leistet. Das Standesamt informiert das Bundeszentralamt für Steuern, das dem Neugeborenen eine grundsätzlich lebenslang gültige Steuer-Identifikationsnummer vergibt (ID). Eine weitere Meldung ergeht an die zuständige kommunale Meldebehörde, die das Neugeborene registriert und eine Meldung an das Finanzamt vornimmt. Für Tot- bzw. Fehlgeburten gibt es gesetzlich vorgegebene Meldewege, bei denen das Standesamt im Mittelpunkt steht.

Bei unverheirateten Eltern wird versucht, die Vaterschaft festzustellen, was mit Einverständnis der Mutter üblicherweise bei dem Jugendamt, dem Amtsgericht oder dem Standesamt erfolgt. Dies dient u. a. der Feststellung der Unterhaltsverpflichtung. Mit der Geburt entsteht ein Anspruch auf Kindergeld, das in der Kommunalverwaltung des Wohnsitzes zu beantragen ist, sowie evtl. auf weitere Hilfen. Bei erwerbslosen Müttern ist zudem die Einschaltung der Deutschen Rentenversicherung relevant.[14]

Das Neugeborene durchläuft direkt nach der Geburt bis zum 6. Lebensjahr mehrere ärztliche Vorsorgeuntersuchungen (U1-U9). Ziel ist es, eine gesunde Entwicklung des Kindes sicherzustellen und insbesondere direkt nach der Geburt erkenn- und behebbare Defizite frühzeitig zu diagnostizieren. Als weiterer Zweck wird angegeben, Hinweise für Kindermisshandlungen zu erhalten und hiergegen vorgehen zu können. Gesetzlich versicherte Kinder haben gemäß § 26 SGB V einen Rechtsanspruch auf Vorsorge. In den meisten Bundesländern soll durch Datenübermittlungen der Meldebehörden und der Kinder- und Jugendärzte die Teilnahme an den Vorsorgeuntersuchungen sichergestellt werden. Eine Pflicht zur Teilnahme an den Untersuchungen besteht jedoch nicht.[15]

Meldeämter, Gesundheitsämter, Sozialleistungsträger, weitere öffentliche Stellen sowie bestimmte private Stellen wie z. B. Arbeitgeber sind verpflichtet,

Daten über die Menschen, mit denen sie zu tun haben, den statistischen Landesämtern bzw. dem Statistischen Bundesamt zu melden. Regelmäßig erfolgt zuvor eine Zusammenführung zu Gruppeninformationen; teilweise werden Einzeldatensätze gemeldet, die dann aber pseudonymisiert werden; eine Rückverfolgung zur konkreten Person soll ausgeschlossen werden und ist unzulässig. Zweck der Statistik ist es ausschließlich, aggregierte gesellschaftlich relevante Daten zu liefern. Mit diesen soll es politischen Entscheidungsträgern erleichtert werden, Planungen vorzunehmen und Strategien zu entwickeln.[16]

Sekundäre Zwecke

Daten aus der Zeit der Schwangerschaft sowie aus der frühkindlichen Entwicklung sind Gegenstand von Forschungsprojekten insbesondere im medizinischen Bereich. Insofern besteht gemäß Art. 5 Abs. 1 lit. b DSGVO ein Recht auf privilegierte Nutzung von ursprünglich für andere Zwecke erhobenen Daten. Voraussetzung ist aber, dass bei der Verarbeitung und Auswertung der Daten geeignete Garantien für den Schutz der Daten getroffen werden (Art. 89 Abs. 1 DSGVO). Solche Garantien bestehen in einer frühestmöglichen Anonymisierung bzw. Pseudonymisierung, in Anzeige- und Genehmigungspflichten, in einer technisch-organisatorischen und räumlichen Abschottung gegenüber sonstigen Zwecken und in einer strengen Zweckbindung.[17]

„Früher war Schwangerschaft ein Zustand – heute ein Projekt". Mit dieser Überschrift wurde eine Studie vorgestellt, in der die Marketingchancen bei werdenden Müttern sowie deren Kommunikations- und Kaufverhalten analysiert wurden. Danach hatte diese Gruppe von Konsumentinnen schon 2011 ein jährliches Umsatzpotenzial von 5 Mrd. Euro. Die Studie kam zu dem Ergebnis, dass Konsum-Entscheidungen von Schwangeren zu langfristigen Bindungen mit Marken und letztlich auch zu einer tiefgreifenden Veränderung ihres Kaufverhaltens führen können.[18] Darin sehen Marketingleute große Chancen, nicht nur für die Hersteller von Umstandsmode und klassischen Babyprodukten, sondern z. B. auch für die Kfz-Industrie, die jungen Familien einen Familien-Van verkaufen möchte. Umwelt- und Gesundheitsaspekte spielen für diese Werbeadressaten eine größere Rolle. Fazit: „Schwangere und frischgebackene Mütter sind eine attraktive Zielgruppe." Diese will erreicht werden. Ein Zugang erfolgt über die Geburtskliniken, in denen mit Willkommenspaketen Nützliches mit Werbebotschaften verbunden wird. Eine Datenweitergabe von der Geburtshilfe an Werber wäre unzulässig, wenn nicht die Betroffenen ihre ausdrückliche Einwilligung erteilt haben.[19]

Für große Internetunternehmen, etwa Google und Facebook, die gemeinsam im globalen Online-Werbebereich inzwischen einen Werbeanteil von 80% erreicht haben, gibt es einfachere Wege, um an sensible Daten über Schwangere und junge Mütter zu gelangen. Sie analysieren das Kommunikations- und Internetnutzungsverhalten z. B. in sozialen Medien und zeigen gegen Entgelt personalisierte Werbung an. Was bei Target im Jahr 2012 noch öffentliche Aufmerksamkeit und Befremden auslöste, erfolgt heute systematisch außerhalb der öffentlichen Wahrnehmung beim Online-Marketing unter Auswertung möglichst vieler im Internet gesammelter Daten – aus Kommunikations- und Suchprofilen, Stichworten, Messenger-Botschaften, „Likes" oder Seitenaufrufen.

Oft sind es die Eltern, die durch unbedachtes Internet-Posting ihren Kindern von Geburt an das Leben schwer machen. Zwar haben die Eltern das Sorgerecht über ihre Kinder und können somit auch über die Verwendung der Daten, etwa in Form von Bildern, teilweise aber auch eigenen Webseiten, auf denen die gesamte Entwicklung für die Welt dokumentiert wird, bestimmen (§ 1626 BGB). Dies ändert aber nichts daran, dass die Kinder eigenständige Rechtssubjekte sind; den Eltern sind Verletzungen des Kindeswohls untersagt. Diese Verletzungen können heute digital erfolgen und die Startbedingungen im Kindergarten, in der Schule und in anderen Lebensbereichen massiv beeinträchtigen.

Big Data?

Die Geburt führt zu informationellen Prozessen. Dabei kommt es zu Datenspeicherungen, die den Menschen das gesamte Leben begleiten können und unterschiedlichsten Zwecken dienen. Sie sind zunächst administrativer Art und verfolgen vorrangig finanzielle und gesundheitliche Ziele. Eine Zusammenführung der Daten erfolgt bisher nicht. Das, was Big Data ausmacht, – die zweckübergreifende Verbindung der Datenbestände mit dem Ziel der Analyse für neue Fragestellungen – ist im Geburtsbereich noch wenig ausgeprägt. Einer solchen Analyse stehen – zumindest in einem gewissen Maße – der Datenschutz bzw. die berufliche Schweigepflicht der medizinischen Dienste entgegen (vgl. Art. 22 Abs. 4 DSGVO).

Die Interessen an den Daten sind aber groß und nehmen zu: Legitim sind Forschungsinteressen, wenn damit wissenschaftliche Fragen beantwortet werden sollen, an deren Beantwortung ein öffentliches Interesse besteht. Legitim sind auch Interessen zur Wahrung des Kindeswohls und zum Schutz der Familie. Solche Datenauswertungen müssen aber in jedem Fall verhältnismäßig sein und dürfen nicht übermäßig in die Rechte von Mutter und Kind eingreifen.

Der Umstand, dass insbesondere durch informationstechnische Unternehmen Daten um die Geburt über Kind und Mutter erhoben werden, gibt Anlass zur Beunruhigung. Die digitale Durchdringung aller Lebensbereiche im Interesse einer kommerziellen Nutzung ist auch hier angekommen. Bei der Werbung gibt es einen fließenden Übergang von sinnvollen gezielten und erwünschten Angeboten zu Manipulation und Ausbeutung. Mutter und Kind dürfen in einer Lebenssituation, in der beide besonders verletzlich und schutzbedürftig sind, nicht zum Objekt von Geschäftemachern werden.

Darum, dass nicht schon zum Lebensbeginn falsche informationelle Weichen gestellt werden, müssen sich alle kümmern: Eltern, die ihrer Fürsorge nachkommen und ihre Verbraucherrechte wahrnehmen, die für den Datenschutz zuständigen Behörden, nicht zuletzt auch die Hebammen und Geburtseinrichtungen sind aufgefordert, illegitime Datenanforderungen zurückzuweisen.

1 Dieser Text ist eine überarbeitete Version eines Beitrags in der Deutschen Hebammen Zeitschrift 2019 (8) 8-13.

2 Matthews/Engel, Der Storch bringt die Babys zur Welt, Stochastik in der Schule 21 (2001), 36-38.

3 Beuth, Big Data: Schwanger ohne digitale Spuren, www.zeit.de. 29.04.2014.

4 Weichert, Big Data im Gesundheitsbereich, 2018, Kap. 4; abrufbar unter http://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf.

5 Z.B. HebRech, Miya, Hebamio, Lucky Midwife, TEMI HEB, Babybamme, HERS-Die.

6 Z. B. GeDoWin Geburt von Staatmann.

7 Weichert, DuD 2002, 137; weitere Nachweise bei Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2015 § 3 Fn. 6.

8 Zilkens, Datenschutz in der Kommunalverwaltung, 3. Aufl. 2011, S. 203.

9 § 3a Embryonenschutzgesetz; Korzilius, Präimplantationsdiagnostik: Der Wunsch nach einem gesunden Kind, www.aerzteblatt.de 2016; 113(33-34); A-1480/B-1249/C-1229.

10 Kassen sollen Tests auf Trisomien finanzieren, SZ 20.09.2019, 6; Janker, Von wegen „guter Hoffnung", SZ 19.09.2019, 4; Schmergal, Der Preis des Wissens, Der Spiegel Nr. 12, 16.03.2019, S. 38 ff.; Ethikdebatte über Bluttests, SZ 23.07.2018, 5 mit Verweis auf Beeck/Henke/Kappert-Gonther/Kober/Rüffer/Schmidt/Schummer/Vogler/Weinberg, Vorgeburtliche Bluttests – wie weit wollen wir gehen?; dazu Berndt, Recht auf Wissen, SZ 18.09.2018, 4.

11 Däubler, Gläserne Belegschaften, 8. Aufl. 2019, Rn. 485, 635; LAG München – 27.09.2017 – 11 TaBV 36/17, ZD 2018, 226; gegen BVerwG 29.08.1990 – 6 P 30/87, NJW 1991, 373; zur Frage nach der Schwangerschaft in einem Bewerbungsverfahren, Däubler, Gläserne Belegschaften, Rn. 215.

12 Gesetz zum Ausbau der Hilfen für Schwangere und zur Regelung der vertraulichen Geburt v. 28.08.2013, BGBl. I S. 3458; kritisch zu früheren Entwürfen Weichert, DANA 3/2003, 7 ff.; zur Anonymität der Schwangerschaftsberatung BVerfG 28.05.1993 – 2 BvF 2/90, 4 u. 5/92, NJW 1993, 1751, 1962.

13 BVerfG 31.01.1989 – 1 BvL 17/87, Rn. 53 f., 65; zu den Rechten des Vaters BVerfG 25.09.2018 – 1 BvR 2814/17.

14 Geburt, https://www.amtlich-einfach.de/DE/Buerger/Familie/Geburt/Geburt_node.html.

15 31. TB ULD Schleswig-Holstein 2009, Kap. 4.5.8; 14. TB SächsDSB 2009, Kap. 10.2.2.; IX. TB LfD LSA 2009, Kap. 21.16; vgl. VerfGH Rheinland-Pfalz 28.05.2008 – B 45/08.

16 Weichert, Big Data im Gesundheitswesen (s. o. En. 4), Kap. 10.7.

17 Weichert in Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 89 Rn. 29-40.

18 https://www.urbia.de/allgemein/presse/frueher-war-schwangerschaft-ein-zustand-heute-ein-projekt.

19 Tekin, Zielgruppe Schwangere und frischgebackene Mütter, www.marketinginwestfalen.de 19.07.2016.

Susanne Holzgraefe

Datenschutz im Kindergarten

Vorwort

Träger von Kindergärten und Kindertagesstätten sind üblicherweise entweder Kirchen, eingetragene Vereine, Stiftungen oder Kommunen. Je nach Träger sind hier unterschiedliche Gesetze und Vorschriften zum Thema Datenschutz zu beachten. Ist die Einrichtung in kirchlicher Hand, so gilt das entsprechende Kirchenrecht. Einrichtungen in staatlicher Hand sind öffentliche Stellen, während Einrichtungen, die von Vereinen oder Stiftungen bereitgestellt werden, nicht-öffentliche Stellen sind. Der Unterschied bezogen auf die Einhaltung der Gesetze und Vorschriften rund um den Datenschutz ist hier allerdings nicht allzu groß.

Betroffene lassen sich in der Regel in sieben Kategorien einteilen:

1. Beschäftigte
2. Kinder
3. Eltern
4. Den Eltern nahestehende Personen
5. Auftragnehmende
6. Personen, die dem Kindergarten Geld oder Sachen spenden
7. Personen, die die Internetpräsentation besuchen

Je nach Träger kann der Kindergarten oder die Kindertagesstätte eine dem Träger untergliederte, eigenständige juristische Person sein. Hier ist in jedem Fall vorab die Verantwortung zum Thema Datenschutz zu klären und vertraglich festzuhalten. Arbeitet die Einrichtung im Auftrag des Trägers oder verarbeitet der Träger die für die Einrichtung anfallenden personenbezogenen Daten im Auftrag? Oder tragen beide die Verantwortung gemeinsam? Sollte der Träger die Verantwortung mit der Einrichtung gemeinsam tragen, sind die Vorschriften der Datenschutzgrundverordnung (DSGVO) für gemeinsame Verantwortliche umzusetzen.

Beschäftigte

Selbstverständlich gelten die Gesetze und Vorschriften zum Thema Datenschutz auch für die Beschäftigten von Kinderbetreuungseinrichtungen. Beschäftigte haben entweder einen Anstellungsvertrag oder eine Beauftragung für eine ehrenamtliche Tätigkeit im Namen der Einrichtung oder des Trägers. In der schriftlich verfassten Beauftragung sollte nicht nur die monetäre Aufwandsentschädigung sondern auch die Tätigkeit genau beschrieben sein. Ehrenamtlich Beschäftigte, die nicht zeitgleich auch Mitglieder der Verantwortlichen sind, gelten als Dritte. Hier ist ein Auftragsverarbeitervertrag abzuschließen.

Auch in Kinderbetreuungseinrichtungen gilt, dass zu Beschäftigten nur personenbezogene Informationen erfasst werden dürfen, die unter Art. 6 Abs. 1 lit. c und d DSGVO fallen. Daten, die zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind (lit. c) oder die die lebenswichtigen Interessen der betroffenen Person oder anderer natürlichen Personen schützen (lit. d). Unter den Schutz von Leib und Leben fallen gesundheitliche Angaben, die unabdingbar sind, um die Kinder vor ansteckenden Krankheiten zu schützen. Darüber hinaus ist natürlich auch erlaubt, Informationen nach Art. 6 Abs. 1 lit. b zu erfassen und zu verarbeiten, sofern es im Anstellungsbeziehungsweise Beauftragtenvertrag entsprechend vereinbart wurde. Üblich ist heutzutage, dass im Arbeitsvertrag eine bargeldlose Zahlung des Gehaltes oder der Aufwandsentschädigung vereinbart wird. In dem Fall ist durch Art. 6 Abs. 1 lit. b DSGVO die Erfassung, Verarbeitung und Weiterleitung der Kontoinformationen erlaubt.

Zu abhängig Beschäftigten, also Beschäftigten, die einen Anstellungsvertrag haben, können keine Informationen erfasst und verarbeitet werden, die unter Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) fallen, da in einem Abhängigkeitsverhältnis die Freiwilligkeit nicht gegeben ist. Für ehrenamtlich Beschäftigte sieht das anders aus. Da sie in keinem Abhängigkeitsverhältnis zur Einrichtung beziehungsweise dem Träger stehen, können hier durchaus freiwillig gegebene Informationen erfasst und verarbeitet werden. Aber auch hier ist die Freiwilligkeit genaustens unter die Lupe zu nehmen. Eine Einwilligung, die unter dem Druck entstanden ist, dass alle Anderen auch einwilligen und sich die betroffene Person bei Nicht-Einwilligung sozial ausgegrenzt fühlt, ist nicht wirksam.

Die Gesetzgebung sieht bei Beschäftigten nicht vor, dass Arbeitgebende Kenntnis von unmittelbaren Kontaktdaten, wie private Telefonnummer oder E-Mail-Adressen, der Beschäftigten haben. Das ist im Bereich der Kinderbetreuungseinrichtung auch wichtig für ehrenamtlich Beschäftigte, denn spätestens, wenn die Verantwortlichen auf die Idee kommen, die Telefonnummern den Eltern weiterzugeben, ist das Risiko, dass die Beschäftigten in ihrer Freizeit belästigt werden, sehr hoch. Aber auch, wenn die Verantwortliche derartige Intentionen nicht verfolgt, ist auch bei Kinderbetreuungseinrichtungen genau wie bei allen anderen Arbeitgebenden das Risiko der Verletzung der Frei- und Ruhezeiten durch Anrufe auf privaten Telefonen durch Vertretende der Verantwortlichen nicht zu unterschätzen. Auch durch die Versendung geschäftlicher E-Mails an private E-Mail-Adressen können sich Betroffene belästigt und in ihrer Frei-, Ruhe- und vor allem Erholungszeit gestört fühlen. Wenn Beschäftigte telefonisch oder per E-Mail erreichbar sein sollen, ist über die Bereitstellung einer E-Mail-Adresse beziehungsweise einer, in der Freizeit abstellbaren, Telefonnummer nachzudenken.

Nicht nur in Kinderbetreuungseinrichtungen, sondern auch bei anderen Vereinen und gemeinnützigen Einrichtungen ist der Trend, dass Beschäftigte ihre eigenen, privaten Smartphones, Laptops und Computer nutzen – Bring Your Own Device (BYOD). Die Gefahren liegen hier auf der Hand. Es müssen Technische und Organisatorische Maßnahmen erstellt werden, die einen vertrauensvollen und sicheren Umgang mit personenbezogenen Daten garantieren. Die Beschäftigten sind Experten in ihren jeweiligen Tätigkeiten, aber ihnen fehlt es häufig an den erforderlichen IT-Kenntnissen, ihre privaten Geräte entsprechend zu gestalten.

Die Einstellung oder externe Beauftragung einer technischen Fachkraft, die sich seitens der Einrichtung beziehungsweise des Trägers um elektronische Geräte, wie Smartphones, Laptops, Arbeitsplatzrechner, Server und so weiter sowie die Umsetzung technischer Maßnahmen kümmert, ist unabdingbar. Hier geht es letztendlich nicht nur um Kinderdaten, sondern häufig auch um gesundheitliche und religiöse Informationen von Kindern aber auch Familien. Die Information, dass die kleine Anna Jüdin und laktoseintolerant ist, ist für die Betreuung beziehungsweise für die Speisezubereitung wichtig zu wissen, hat aber dennoch nichts auf dem privaten Laptop der Erziehenden beziehungsweise der Köche oder gar in Google Docs oder bei WhatsApp verloren und sollte auch nicht einfach so unverschlüsselt über die Internetverbindung eines privaten Haushaltes kommuniziert werden. Organisatorische Maßnahmen wie Betriebsanweisungen sind hier zwingend erforderlich.

Personalakten und Akten von ehrenamtlich Beauftragten sollten auch in Kinderbetreuungseinrichtungen nicht offen herumliegen. Sie sind unter Verschluss zu halten. Inwieweit die Leitung der Einrichtung die Befugnis der Einsicht der Personalakte hat, hängt vom Vertrag und der juristischen Konstellation der Einrichtung zum Träger ab.

Schichtpläne, aus denen die Identität der einzelnen Beschäftigten erkennbar ist, sollten nicht in Fluren hängen, zu denen alle Eltern Zutritt haben. Das gilt auch für die Urlaubsplanung und Krankmeldungen von Beschäftigten.

Stempeluhren, die zur Festhaltung der Anwesenheitszeiten von Beschäftigten den Fingerabdruck der Beschäftigten scannen, sind zu überdenken. Hier lassen sich mildere Mittel finden, bei denen nicht der Fingerabdruck gespeichert wird.

Ehrenamtlich Beschäftigte sind, je nach Zugehörigkeit zur Einrichtung beziehungsweise zum Träger, als Beschäftigte oder Dritte zu sehen. Organisatorische Maßnahmen, wie die Verpflichtung auf Vertraulichkeit, sollten auch von Ehrenamtlern unterschrieben werden. Auch sollte sichergestellt werden, dass Ehrenamtler nachweislich nicht nur Kenntnis von allen Betriebsanweisungen haben, sondern sich auch verpflichten, sich an die Anweisungen zu halten.

Kinder

Natürlich sollte die Betreuungseinrichtung nicht nur den Namen des Kindes wissen, sondern auch das Alter beziehungsweise das Geburtsdatum, wo das Kind wohnt, wer die Eltern sind und was sonst an Informationen für eine ordnungsgemäße Betreuung zwingend erforderlich ist. Das sind Informationen, die aus dem Betreuungsvertrag hervorgehen sollten. Die Rechtsgrundlage liefert Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung). Da die zu betreuenden Kinder teilweise in einem Alter sind, in dem sie sich noch nicht selbst durch Sprache identifizieren können, ist es hier durchaus sinnvoll, dass auch

die Erfassung und regelmäßige Aktualisierung von Fotos des Kindes Vertragsbestandteil ist, damit die Erziehenden und Betreuenden die Kinder identifizieren können.

Darüber hinaus sind je nach Betreuungsumfang auch noch Informationen entsprechend Art. 6 Abs. 1 lit. d (Leib und Leben) erforderlich, wie Informationen zur Gabe von Medikamenten, körperliche Einschränkungen wie Seh- oder Hörschwächen, Allergien, Schwimmerfahrung und so weiter. Auch die Angabe von unmittelbaren Notfallkontaktdaten von drei priorisierten Personen könnte mit lit. d begründet werden, sofern es nicht schon mit lit. c (Vertragserfüllung) begründet wurde.

Die Kinder in Kindergärten und Kindertagesstätten sind in der Regel unter sechs Jahre alt. Daher gestaltet sich das mit der Einwilligung etwas schwieriger. Es ist die Frage, was für Informationen werden von Kindern erhoben, die einer Einwilligung bedürfen. Das sind in der Regel Foto- und Videoaufnahmen. Nein sollte immer Nein bleiben. Egal was die Eltern sagen, wenn das Kind Nein sagt, ist es Nein. Wenn das Kind ‚Ja' sagt, ist die Einwilligung aller Erziehungsberechtigten erforderlich. Die Einrichtungen werden hier gerne zum Spielball in Scheidungskriegen. Ein Elternteil stimmt zu, das andere fühlt sich übergangen und zeigt die Einrichtung wegen Nicht-Einholung der Einwilligung an. Solange keine schriftliche Vollmacht des anderen Erziehungsberechtigten vorliegt, dass der eine Erziehungsberechtigte allein entscheiden darf, ist es ratsam, Einwilligung von allen Erziehungsberechtigten einzuholen. Anders als für medizinische Untersuchungen, gibt es hier noch keine höchstrichterlichen Urteile, die besagen, dass es in Ordnung ist, wenn nur ein Erziehungsberechtigter zustimmt.

Dürfen die Erziehenden mit den Kindern in den Gruppen Adressen üben? Die Beschwerde der Eltern ist hier, dass die Kinder auf diese Weise die Adressen der anderen Kinder erfahren. Hier gilt es natürlich abzuwägen, wie wichtig es ist, dass das Kind seine eigene Adresse lernt, damit es im Notfall auch nach Hause findet. Die Kinder tauschen untereinander noch viel sensiblere Daten aus. So erzählt der kleine Paul dem kleinen Simon stolz, dass er laktoseintolerant ist, weil er stolz ist, dass er das Wort endlich behalten hat. Die Kinder, die tagtäglich miteinander in der Gruppe sind, bekommen auch mit, welches Kind eine Sehschwäche hat, welches Kind koscher isst, welches vor zwei Wochen Windpocken hatte und so weiter. Es sollte hier Aufgabe der Eltern sein, den eigenen Kindern beizubringen, dass sie nicht in der ganzen Nachbarschaft herumerzählen, dass Klara Scharlach hatte. Aber natürlich sollte es auch Aufgabe der Erziehenden sein, die Kinder für den Respekt der Privatsphäre und Privatheit zu sensibilisieren.

Das Schöne an Kindergärten ist, dass in der Regel in den Fluren nicht die Namen der Kinder an Jackenhaken und Ablagen hängen, sondern Bilder. Dass der Hase für Paul Müller und die Maus für Eva Meier steht, ist für Besuchende nicht erkennbar. Das könnte als eine Form der Pseudonymisierung gesehen werden, die schon seit über fünfzig Jahren existiert.

Die Einrichtungen sollten sich überlegen, ob Köche oder das externe Catering unbedingt wissen müssen, dass Anke Jansen laktoseintolerant ist, Maja Müller koscher isst, Frank Paulsen eine Nussallergie hat und Otto Pieper unter Zöliakie leidet oder ob es reicht, wenn die Betreuenden diese Informationen kennen und nur an die Küche weitergegeben wird: heute 3x laktosefrei, 2x Nussallergie, 1x Zöliakie und 2x koscher. Ist es hier wirklich zwingend erforderlich, die Identität der Kinder weiterzugeben? Zumal hier nicht nur die Identität weitergegeben wird, sondern auch die Information, wann das Kind anwesend ist. Die Küche kann bei Angabe der Namen einfach herausfinden, welche Kinder an welchen Tagen nicht in der Einrichtung sind.

Foto- und Videoverbot

Zu Fotos von Kindern gibt es einen gesonderten, ausführlichen Artikel. Die Einrichtung beziehungsweise der Träger der Einrichtung ist für alle Fotos, Video- und auch Audioaufzeichnungen verantwortlich, die auf dem Gelände der Einrichtung aufgenommen werden. Wenn also die Oma die Gruppe spielender Kinder fotografiert und im sozialen Netzwerk postet, ist die Einrichtung beziehungsweise der Träger verantwortlich. Wenn der Zaungast ein Foto von spielenden Kindern auf dem Spielplatz des Kindergartens macht und veröffentlicht, ist der Kindergarten beziehungsweise sein Träger verantwortlich. Daher ist es ratsam, wenn die Einrichtungen das Fotografieren und Filmen auf ihrem Gelände verbieten. Es ist ratsam Schilder mit durchgestrichenen Kameras sichtbar aufzuhängen. Auch Audioaufnahmen sollten verboten werden. Wenn dann doch von einer Veranstaltung Fotos gemacht werden sollen, dann hat der Verantwortliche immer noch die Möglichkeit, Fotografen zu akkreditieren, die die Datenschutzbestimmungen beachten.

Eltern beziehungsweise Erziehungsberechtigte

Kindergärten und Kinderbetreuungseinrichtungen erheben und verarbeiten natürlich auch personenbezogene Daten von Eltern beziehungsweise Erziehungsberechtigten. Hier werden Daten angefragt, wie Namen, ladungsfähige Anschriften, unmittelbare Kontaktmöglichkeiten und, sofern die bargeldlose Zahlung vereinbart wurde, auch das SEPA Mandat und was sonst noch für den Betreuungsvertrag zwingend erforderlich ist. Die rechtliche Grundlage ergibt sich wieder aus Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung). Selbstverständlich sollte es der Einrichtung auch freistehen, bei der Anmeldung einen Nachweis über die Erziehungsberechtigung zu fordern. Um spätere Überraschungen zu vermeiden, sollte die Einrichtung Kenntnis über die Identität aller Erziehungsberechtigten haben. Um den Erziehungs- und Betreuungsablauf möglichst unkompliziert zu gestalten, und bei späteren Einwilligungen nicht hinter allen Erziehungsberechtigten hinterher zu laufen, ist es ratsam, wenn die Erziehungsberechtigten sich gegenseitig bevollmächtigen, oder zumindest der eine dem anderen eine schriftliche Vollmacht erteilt, dass bei Entscheidungen, wie Einwilligungen, die Zustimmung des einen Erziehungsberechtigten ausreicht. Die Erhebung und Verarbeitung von regelmäßig aktualisierten Fotos der Erziehungsberechtigten hilft

den Erziehenden und Betreuenden bei der schnelleren Zuordnung von Kind zu Eltern. Die Alternative wäre im Zweifel das Vorzeigen eines gültigen Lichtbildausweises.

Der Vertrag sollte darüber hinaus auch von den Erziehungsberechtigten gegebene Angaben erhalten, wer im Notfall wie kontaktiert werden kann. Es ist zu empfehlen, hier die unmittelbaren Kontaktdaten, wie Festnetz- und Mobilfunknummer von drei priorisierten, verschiedenen Personen anzugeben, so dass es, falls die Person mit der höchsten Priorität nicht erreicht werden kann, noch zwei weitere Personen als Backup gibt. Auch hier muss die Einrichtung die Möglichkeit haben, die Personen zu identifizieren. Eine Möglichkeit wäre, im Vertrag festzuhalten, dass die Personen im Zweifel einen Lichtbildausweis vorzeigen müssen. Eine andere Möglichkeit wäre, über die Erziehungsberechtigten aktuelle und in regelmäßigen Abständen aktualisierte Fotos der Notfallkontaktpersonen zu erheben und zu verarbeiten.

Wichtig ist in diesem Zusammenhang, dass die Personen, die durch die Erziehungsberechtigten als Notfallkontakte angegeben werden, schriftlich entsprechend Art. 14 DSGVO informiert werden. Das kann auf dem postalischen Weg passieren oder durch eine persönliche Aushändigung.

Wenn ein Kindergarten oder eine Kindertagesstätte den Eltern oder Erziehungsberechtigten wichtige Informationen zukommen lassen möchte, kann das natürlich über die Überreichung in Papierform bei der Abholung oder klassisch auf dem Postweg passieren, oder per E-Mail. Die Erhebung der E-Mail-Adresse ist dafür erforderlicher Vertragsbestandteil. Hierüber dürfen aber nur Informationen verteilt werden, die für den Betriebsablauf erforderlich sind. Wie zum Beispiel, dass ein Ausflug oder ein Theaterstück geplant ist. Werbung mit dem Ziel, mehr Anmeldungen oder Spenden zu erhalten, dürfen auch Kindergärten und Kindertagesstätten nur dann an die Eltern versenden, wenn die Eltern explizit eingewilligt haben.

Selbstverständlich sind unmittelbare Kontaktmöglichkeiten der Eltern und Erziehungsberechtigten, wie Telefonnummern und E-Mail-Adressen, vertraulich zu behandeln und dürfen nur verwendet werden, wenn es wegen des Kindes einen akuten Klärungsbedarf gibt. Generell empfinden viele Menschen unangekündigte Telefongespräche als Belästigung. Wenn die Klärung mehr als 30 Minuten Zeit hat, ist es empfehlenswert, wenn die Einrichtung eine Textnachricht (SMS) mit der Bitte um ein Telefonat dem Anruf vorausschickt. Hierbei ist auf das Medium zu achten. Die Nutzung von Elterndaten via WhatsApp ist nicht zulässig. Hat die Klärung Zeit bis zum nächsten Tag, ist hier die Versendung einer E-Mail zu empfehlen. Bei der Verwendung von E-Mails ist auf Verschlüsselung zu achten. Alternativ lässt sich ja auch eine Nachricht auf Papier dem Kind beziehungsweise dem Abholenden mitgeben.

Der Prozess, wie ein Kind für einen oder mehrere Tage Abwesenheit zu melden ist, sollte ebenfalls im Vertrag festgelegt sein. Es ist hier zu bedenken, dass die Einrichtung natürlich über ansteckende Krankheiten eines Kindes oder in der Familie eines Kindes Bescheid wissen muss.

Es ist zu empfehlen, dass Elternvernetzung nicht durch die Einrichtung vorgenommen wird, sondern in Eigeninitiative der Eltern.

Den Eltern nahestehende Personen

Den Eltern beziehungsweise den Erziehungsberechtigten nahestehende Personen, von denen die Einrichtungen personenbezogene Daten erheben und verarbeiten, sind zum Beispiel Personen, die berechtigt sind, das Kind abzuholen oder auch Personen, die mit dem Kind an Stelle der Eltern an einer Veranstaltung teilnehmen. Die Beschäftigten der Einrichtung müssen die Personen eindeutig identifizieren können.

Die Daten werden durch die Eltern beziehungsweise die Erziehungsberechtigten erhoben. Name, ladungsfähige Anschrift sowie unmittelbare Kontaktmöglichkeit sind üblich. Wie oben schon beschrieben, ist es hier hilfreich, wenn die Erziehungsberechtigten ein aktuelles Foto der Person einreichen, das regelmäßig aktualisiert wird, um die Überprüfung durch einen Lichtbildausweis zu vermeiden.

Es sollte Aufgabe der Eltern sein, die betroffenen Personen über die Datenweitergabe zu informieren. Es ist die Pflicht der Einrichtung beziehungsweise des Trägers, hier die betroffenen Personen entsprechend Art. 14 DSGVO zu informieren. Das kann über den Postweg passieren oder durch eine die persönliche Aushändigung.

Auftragnehmende

Auftragnehmende, die im Auftrag personenbezogene Daten verarbeiten, können aus unterschiedlichen Bereichen kommen. Das kann der Caterer sein, das kann aber auch der selbständige Erzieher sein oder der ehrenamtliche Betreuer, der kein Mitglied im Verein der Einrichtung ist. Es kann aber auch der externe IT-Dienstleister sein.

Die Frage, die hier häufig gestellt wird: Das ist doch B2B, wo greift denn hier die DSGVO und andere Gesetze und Vorschriften zum Datenschutz? Bei Ein-Personen-Unternehmen hat natürlich die eine Person das Recht auf die Wahrung ihrer Persönlichkeitsrechte. Das gilt auch für Beschäftigte von anderen Unternehmen. Zum Beispiel unterliegen die direkten Kontaktdaten von Beschäftigten eines Auftragnehmers der DSGVO. Der Umgang mit Daten von selbständigen oder ehrenamtlichen Erziehenden beziehungweise Betreuenden sollte sich nicht groß vom Umgang mit den Informationen zu Beschäftigten unterscheiden. Was allerdings erforderlich ist, ist Auftragsverarbeiterverträge entsprechend Art. 28 DSGVO abzuschließen. Je nach Größe des Unternehmens ist es ratsam, auch mit der Nutzung von Telefonnummern vorsichtig umzugehen.

Geld- und Sachspendende

Die Erfassung von personenbezogenen Daten von Spendern ist nur dann erforderlich, wenn die Spendenden einen Nachweis über ihre Spende verlangen oder die Spende in einer Höhe ist, dass der Name des Spendenden bekannt gegeben werden muss. Bei einer Spende ist es immer ratsam, nachzuhaken, ob die Person einen Nachweis, eine Quittung, haben möchte oder die Spende als anonyme Spende verbucht werden soll. Wird ein Nachweis verlangt, so wird die Steueridentifikationsnummer des Spenders benötigt. Alternativ hat der Spen-

der seinen Namen und seine postalische Anschrift mitzuteilen. Die Rechtsgrundlage ergibt sich aus Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Vorgabe).

Spenderdaten dürfen natürlich nur für die Buchhaltung verwendet werden. Spendern hier ohne explizite Einwilligung Werbung zukommen zu lassen, ist nicht zulässig.

Besuchende der Internetpräsentation

Auch Webseiten von Kinderbetreuungseinrichtungen sollten DSGVO-konform gestaltet werden. Es ist hier nicht ratsam, einen hausbackenen Auftritt ins Netz zu stellen. Hier sind einige Fallstricke zu beachten. Häufig wird nicht nur die IP-Adresse erhoben und durch den Webserver-Dienstleister, mit dem es einen Auftragsverarbeitervertrag geben sollte, sieben Tage gespeichert, sondern es werden Betreuungsanträge zum Download oder gar zur Online-Ausfüllung angeboten und so weiter. Eventuell wird sogar mit Kinderfotos geworben.

Hier sind einige organisatorische Maßnahmen erforderlich, die bedacht werden müssen. Liegen Einwilligungen der abgebildeten Personen auf den Fotos vor? Für wie lange gelten die Einwilligungen? Kaum ein Kind möchte auch noch nach fünfzig Jahren sein Foto unhonoriert auf der Schokoladenpackung sehen. Die Informationen entsprechend Art. 13 DSGVO (im Volksmund Datenschutzerklärung genannt) für Internetpräsenzen sind vorzuhalten.

Löschpflichten

Wann ist die Einrichtung beziehungsweise der Träger verpflichtet, die Daten zu löschen? Für die Spenderdaten gelten die Vorschriften des Steuerrechts. Für die Verträge gelten die Aufbewahrungsfristen des Handelsgesetzbuches. Alles andere ist zu löschen, sobald es nicht mehr benötigt wird. Wenn das Kind eingeschult wird, benötigt der Kindergarten die Information, dass es laktoseintolerant ist, nicht mehr. Derartige Informationen sollten umgehend vernichtet werden. Auch die Information, wer das Kind abholen durfte, ist dann nicht mehr von Belang und zu vernichten.

Recht auf Datenübertragbarkeit

Betroffene haben das Recht auf Datenübertragbarkeit. Das würde zum Beispiel bedeuten, dass, wenn das Kind die Betreuungseinrichtung wechselt, die Erziehungsberechtigten die Daten in einem maschinenlesbaren Format anfordern können, die dann von der neuen Betreuungseinrichtung eingelesen und verarbeitet werden sollen.

Es ist hier zu bezweifeln, dass die Einrichtungen zum heutigen Zeitpunkt überhaupt schon so weit sind. Vieles passiert noch auf Papier. Auch bietet eventuell verwendete Software gar keine Kompatibilitätsmöglichkeit zur verwendeten Software der neuen Einrichtung. Wenige Softwarehersteller haben sich bereits um die Implementierung entsprechender Schnittstellen bemüht.

Recht auf Kopie der Daten

Betroffene haben das Recht auf eine Kopie ihrer Daten. Eltern beziehungsweise Erziehungsberechtigte natürlich auch für die Daten ihrer Kinder. Über die genaue Form der Kopie lässt sich die DSGVO nicht eindeutig aus. Die DSGVO sagt nur, dass die Kopie in elektronischer Form zu erfolgen hat, wenn der Antrag elektronisch gestellt wurde. Sie lässt sich aber nicht darüber aus, in welcher Form die Kopie zu erfolgen hat, wenn der Antrag in anderer Form gestellt wird. Es kann hier auch nicht vom Verantwortlichen verlangt werden, elektronisch vorliegende Daten auf Papier auszudrucken, denn dann wäre es keine Kopie, sondern ein Ausdruck. Elektronisch vorliegende Daten können nur elektronisch kopiert werden. Daten, die auf Papier vorliegen, können entweder eingescannt oder auf Papier kopiert werden. Werden die Daten jedoch eingescannt, ist zu beachten, dass sie dann elektronisch vorliegen und dafür die technischen und organisatorischen Maßnahmen angepasst werden müssen.

Datenschutzbeauftragte

Müssen Kindergärten und Kindertagesstätten eine Datenschutzbeauftragte bestellen? Die Träger von Kinderbetreuungseinrichtungen sind meistens so groß, dass sie in jedem Fall eine oder gar mehrere Datenschutzbeauftragte bestellt haben, die dann natürlich auch für die Kindergärten und Kindertagesstätten mit zuständig sind. Ist die Einrichtung eine eigenständige, juristische Person, ist sie in der Regel nicht so groß, dass sie eine Datenschutzbeauftragte bestellen müsste. Eine Datenschutzexpertin beratend an der Seite zu haben, ist empfehlenswert, da gerade in Kinderbetreuungseinrichtungen von Seiten der Eltern viel Halbwissen verbreitet wird.

In eigener Sache

DANA-Preise ab 2020

Seit 2014 betrug der Preis der Datenschutz Nachrichten unverändert 12,00 Euro. Durch höheren Umfang und höhere Produktionskosten steigt der Heftpreis ab 01.01.2020 auf 14,00 Euro. Die Abopreise erhöhen sich auf 48,00 Euro für 4 Ausgaben pro Jahr in Deutschland. Abonnenten aus dem Ausland zahlen zukünftig 58,00 Euro.

Mitgliedsbeiträge ab 2020

Die normalen Mitgliedsbeiträge steigen von 75,00 Euro auf 90,00 Euro/Jahr. Die ermäßigten Beiträge steigen von 32,00 Euro auf nunmehr 36,00 Euro/Jahr. Der Mindestbeitrag für Firmenmitgliedschaften steigt von 160,00 Euro auf 185,00 Euro/Jahr.

Susanne Holzgraefe

Datenschutz im offenen Ganztag

Vorwort

Offene Ganztagsschulen sind der Trend in manchen Gegenden. Gerade in wenig bevölkerten Regionen kommt es immer häufiger vor, dass die einzige Schule eine offene Ganztagsschule ist. Die Eltern entscheiden hier, ob das Kind Mittagessen und eine Nachmittagsbetreuung erhält oder nach dem Unterricht nach Hause geht. Einmal festgelegt, lässt es sich an vielen Schulen im laufenden Schuljahr nicht ändern. Entweder an jedem Schultag Mittagessen und Nachmittagsbetreuung oder gar nicht.

Die Essenversorgung und die Betreuung wird häufig nicht von der Schule sondern von externen Vereinen oder anderen Organisationen sowie externen Catering-Firmen durchgeführt. Hierbei fallen natürlich einige personenbezogene Daten an. Nicht selten bekommt das Catering direkt die Information, dass Maik Schlüter laktoseintolerant ist, Frauke Rothschild koscher isst und Fritz Herrmann unter Zöliakie leidet. Auch kann es vorkommen, dass hier direkt an die Catering-Firmen weitergegeben wird, dass Peter Meier und Anke Müller heute krank sind und daher kein Mittagessen für sie geliefert werden braucht.

Die Betreuenden der hier beschriebenen offenen Ganztagsschulen sind entweder bei dem Verein oder der Organisation angestellt, als Mitglieder ehrenamtlich tätig oder extern ehrenamtlich oder als Selbständige beschäftigt. Sie bekommen personenbezogene Informationen entweder von der Verwaltung der Vereine und Organisationen oder direkt von der Schule. Die Vereine und Organisationen bekommen personenbezogene Daten entweder von der Schule, vom Jugendamt oder durch direkte Erhebung bei den Eltern. Ein Standard-Verfahren gibt es hier nicht.

Die Betreuung selbst findet entweder direkt in der Schule oder auf dem Gelände der betreuenden Vereine und Organisationen statt.

Verantwortliche

Als erstes stellt sich bei offenen Ganztagsschulen die Frage, wer ist verantwortlich für die für die Betreuung und die Essenversorgung anfallenden personenbezogenen Daten? Die Schule, die Kommune, das Bundesland, der betreuende Verein beziehungsweise die betreuende Organisation, die Catering-Firma oder wurden hier gemeinsam Verantwortliche entsprechend Art. 26 DSGVO festgelegt? Oder wurde mit dem betreuenden Verein beziehungsweise der betreuenden Organisation eine Verarbeitung im Auftrag entsprechend Art. 28 DSGVO vertraglich vereinbart? Und wer ist verantwortlich für die Beauftragung des Catering?

Hier gilt es in jedem Fall die Verträge genau zu prüfen. Auch stellt sich die Frage, ob es wirklich das mildeste Mittel ist, personenbezogene Kinderdaten an das Catering-Unternehmen weiterzuleiten. Reicht es nicht, wenn die Betreuenden wissen, welches Kind Esseneinschränkungen hat. Reicht es nicht, täglich der Catering-Firma mitzuteilen: heute 184 mal normal, 5 mal koscher, 18 mal laktosefrei und 34 mal Nussallergie. Muss die Catering-Firma wirklich die Namen der Kinder auf die Essenportionen schreiben? Kann die Verteilung der Spezialessen nicht durch die Betreuenden erfolgen?

Werden Daten an die Catering-Firma weitergeleitet, so ist darauf zu achten, dass die Catering-Firma ein Auftragsverarbeiter ist und hier Art. 28 DSGVO einzuhalten ist.

Beschäftigte

Der Beschäftigten-Datenschutz ist natürlich auch hier einzuhalten. Neben Beschäftigten mit Anstellungsvertrag, kann es ehrenamtliche Beschäftigte geben, die als Mitglieder des Vereins oder der Organisation ehrenamtlich (gegen Aufwandsentschädigung) tätig sind. Da sie durch die Mitgliedschaft eine direkte Zugehörigkeit zum Verein haben, sind es keine Dritten.

Dritte sind jedoch Beschäftigte, die selbständig sind und vom Verein beziehungsweise der Organisation beauftragt werden, sowie ehrenamtlich Beschäftigte, die keine Mitglieder des Vereins oder der Organisation sind. Sofern personenbezogene Daten an sie weitergeleitet werden, was sich bei der Kinderbetreuung schwer ausschließen lässt, sind sie Auftragsverarbeiter und es sind die Bestimmungen entsprechend Art. 28 DSGVO einzuhalten.

Transparenz

Es ist darauf zu achten, dass die Kinder und Jugendlichen sowie die Eltern beziehungsweise die Erziehungsberechtigten alle Informationen entsprechend Art. 13 und Art. 14 DSGVO erhalten. Die Informationen sollten entsprechend Art. 12 DSGVO klar und leicht verständlich und in möglichst einfacher Sprache verfasst sein und es sollte gegebenenfalls mit Piktogrammen und Bildern gearbeitet werden. Das Augenmerk sollte darauf gelegt werden, dass die Kinder die ihnen ausgehändigten Informationen verstehen.

Rechtsgrundlagen

In der offenen Ganztagsbetreuung werden einige Daten erhoben und verarbeitet, die zur Vertragserfüllung erforderlich sind. Die Rechtsgrundlage bietet hier Art. 6 Abs. 1 lit. b DSGVO. Lebensnotwendige Informationen wie zum Bespiel gesundheitliche Esseneinschränkungen, wie häufig das Kind welche Medikamente benötigt oder ob und wie gut das Kind schwimmen kann, können mit Art. 6 Abs. 1 lit. d DSGVO begründet werden.

Einwilligungen gestalten sich als schwierig, da die Freiwilligkeit stets genausten unter die Lupe genommen werden sollte. Steht der Jugendliche wirklich nicht unter dem sozialen Druck,

einzuwilligen, weil alle Anderen auch eingewilligt haben?

Soziale Netzwerke

Eltern, aber auch Kinder und Jugendliche möchten sich gerne in sozialen Netzwerken organisieren. Betreuende Vereine und Organisationen sind gut beraten, hier keine Initiativen zu ergreifen und sich an derartigen Organisationen nicht zu beteiligen. Wenn sich Eltern oder Kinder und Jugendliche untereinander organisieren möchten, dann privat und nicht unter der Verantwortung der Betreuenden.

Auch ist es wünschenswert, dass Betreuende Kinder und Jugendliche auf Datenschutz und die Nutzung von sozialen Netzwerken regelmäßig sensibilisieren. Die Erfahrungen zeigen, dass Kinder und Jugendliche häufig unbedacht Fotos, Videos und auch Tonaufnahmen von anderen Kindern und Jugendlichen ins Netz posten, unverschlüsselt miteinander chatten oder E-Mails austauschen und ihr eigenes komplettes Leben im Netz öffentlich machen. Wie groß hier die Gefahren sind, können sie dabei noch gar nicht abschätzen. Stetiges Sensibilisieren durch Erziehende, Lehrende, Betreuende und andere ist hier wichtig.

Technische und Organisatorische Maßnahmen

Werden Informationen an Betreuende weitergeleitet, so ist sicherzustellen, dass die Informationen bei den Betreuenden vertraulich verarbeitet werden. Sollten Betreuende für die Speicherung technische Geräte nutzen, so müssen selbstverständlich auch hier technische Maßnahmen ergriffen werden, damit die Daten sicher abgelegt werden und die Vertraulichkeit bei der Verarbeitung nicht (unbewusst) verletzt wird.

Es ist ratsam, dass die Vereine und Organisationen mindestens eine Person beschäftigt haben, die sich um die Sicherheit der technischen Geräte sowie der Server kümmert. Die Träger sollten ihre Beschäftigten in den Umgang mit verschlüsselter Kommunikation einweisen. Regelmäßiges Sensibilisieren der Beschäftigten, nicht nur auf Datenschutz sondern auch auf Datensicherheit, ist ratsam.

Fazit

Der Unterschied beim Datenschutz im offenen Ganztag zum Datenschutz im Kindergarten ist, dass die Kinder älter sind. Sie können mit zunehmendem Alter immer besser lesen und schreiben, nutzen immer mehr technische Geräte und neue Techniken, um sich mit der Welt zu vernetzen. Aufklärung und Sensibilisieren ist hier von enormer Wichtigkeit. Die Kinder und Jugendlichen sollten dabei auch die Grenzen der eigenen Privatheit entdecken und schätzen lernen.

Michael Schlegel, Tobias Straub

„Das hätte ich nicht gedacht, dass es so einfach ist an die Daten zu kommen.“ – Praktische Sensibilisierung an Schulen

Die bezeichnende Aussage im Titel stammt aus dem Kreis der Schülerinnen und Schüler, die jüngst an einem unserer Hands-on Workshops zur Datenschutz-Sensibilisierung teilnahmen. Dieser Beitrag umreißt die hierfür nötigen Vorarbeiten und die bei der Durchführung gewonnenen Erkenntnisse.

Verwandte Ansätze und Motivation

Beispielgebend für die Sensibilisierung an Schulen und hinsichtlich ihrer Reichweite führend dürfte die Initiative „Datenschutz geht zur Schule“ des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. sein. Bereits seit 2009 engagieren sich Mitglieder ehrenamtlich, um bundesweit Sensibilisierungsvorträge anzubieten. In 90-minütigen Einheiten werden anhand praktischer Beispiele und Videoclips Risiken und Verhaltensregeln für typische Anwendungsfälle von Kindern und Jugendlichen erklärt.[1]

Der Bevölkerung Datenschutz auch einmal auf unkonventionelle und Aufsehen erregende Weise näher zu bringen, ist Teil des vom Landesbeauftragten Baden-Württemberg formulierten Konzepts „Datenschutz als KULTuraufgabe“, das das Anliegen des Schutzes personenbezogener Daten künstlerisch vermitteln soll. Aus unserem Kontakt mit der Aufsichtsbehörde entstand die Idee, mit Studierenden Demonstratoren zu entwickeln, die möglichst plastisch Auswirkungen der Datenverarbeitung verdeutlichen. Dadurch sollten die oft nur abstrakt wahrgenommenen Risiken stärker ins Bewusstsein gerückt werden, um dem als „privacy paradox“ bekannten Phänomen entgegen zu wirken und tatsächlich Verhaltensänderungen anzustoßen.

Einbindung von Studierenden

Das Curriculum des Bachelor-Studiengangs Wirtschaftsinformatik an der Dualen Hochschule Baden-Württemberg (DHBW) sieht vor, dass sich alle Studierende im dritten Jahr in einem Projekt intensiv mit einer Fragestellung auseinandersetzen, um insbesondere ihre Fähigkeiten zur Teamarbeit und Kenntnisse des Software Engineerings zu vertiefen. Im Wintersemester

2017/18 entstanden dabei anfänglich vier Android Apps sowie eine Anwendung für den Einplatinenrechner Raspberry Pi, die jeweils die technische Machbarkeit zeigten. Vorgabe für eine sich im Sommersemester anschließende Wahlvorlesung war es, die Ergebnisse aufzubereiten und in geeigneter Weise der Öffentlichkeit vorzustellen. Die Studierenden entschieden sich dabei für SchülerInnen als Zielgruppe und konzipierten eine Sensibilisierungsveranstaltung für ein Stuttgarter Gymnasium, für die sie zwei der entwickelten Apps einsetzten.

In ähnlicher Weise wiederholten wir im Folgejahr das Format der Lehrveranstaltungen mit wachsender Beteiligung, wobei die beiden Apps weiterentwickelt und durch sechs neue Anwendungen ergänzt wurden.[2] Als Vorgehensmodell zur Softwareentwicklung gaben wir dabei erstmals Scrum und entsprechende technische Hilfsmittel als verpflichtend vor, um die Effizienz zu steigern.

Konzept der Workshops an Schulen

Die den Schulen als „Datenschutztag" angebotene Veranstaltung ist für eine Gesamtdauer von ca. drei Stunden und für 15 bis 50 TeilnehmerInnen ab der 7. Jahrgangsstufe ausgelegt. Als Lernziele sollten die SchülerInnen – anhand der Diskussion über Videoüberwachung – erfahren, welcher Überwachung sie im Alltag ausgesetzt sind und es sollte ihnen andererseits verdeutlicht werden, welche Gefahren mit mobilen Anwendungen verbunden sein können.

In den Workshops treten dabei ausschließlich Studierende[3] als ReferentInnen auf, da wir annehmen, dass diese aufgrund des geringeren Altersunterschieds für die Zielgruppe nahbarer und damit glaubhafter wirken.

Nach einer kurzen Einführung werden aus drei bis fünf SchülerInnen bestehende Teams gebildet, die jeweils wenigstens über ein hinreichend aktuelles Android-Smartphone verfügen müssen. Auf diesem wird unsere App Camfinder verwendet, mit der die Kartendaten des Community-Projekts Surveillance under Surveillance[4] visualisiert und selbst ergänzt werden können. Letzteres ist das Ziel einer anderthalbstündigen „Challenge" in Form einer Stadtrallye, bei der es gilt, möglichst viele Überwachungskameras zu finden und zu dokumentieren.

Bei der zweiten App, die an die SchülerInnen für die Dauer der Veranstaltung verteilt wird, handelt es sich dagegen um Spionagesoftware, die eine Fernsteuerung eines Smartphones erlaubt. Die Schadfunktionen werden dabei durch eine plausible „cover story" verschleiert. Wahlweise wird dabei bFree als leistungsfähiger Virenscanner oder WhiteHatChat als sicherer Messenger angeboten.

Nach Auswertung der Ergebnisse der Rallye, bei der typischerweise (im innerstädtischen Bereich) eine für die SchülerInnen erstaunlich hohe Zahl von Kameras gefunden wird, erfolgt schließlich auch die Offenlegung der Spionagesoftware. Dabei wird die Administrator-Oberfläche der Serverkomponente gezeigt, über die die verbundenen Geräte etwa angewiesen werden können, Positionsdaten zu sammeln, Kontakte auszulesen, heimliche Tonaufnahmen und Fotos zu machen oder SMS in fremdem Namen zu versenden.

Bei der Darstellung des technisch Machbaren wird behutsam vorgegangen und konsequent auf einen respektvollen Umgang geachtet. Um niemanden bloßzustellen, werden die ausspionierten Informationen verschlüsselt gespeichert und nur der betroffenen Person selbst zugänglich gemacht. Vor der Gruppe werden nur solche Aufzeichnungen gezeigt, die über ein Vorführgerät der DHBW gewonnen wurden und keine unbeteiligten Dritten tangieren.

Zwei kurze Videoclips, die fiktiv den wirtschaftlichen bzw. kriminellen Missbrauch personenbezogener Daten illustrieren, und Hinweise zum Selbstschutz leiten zur abschließenden Diskussion über.

Lessons Learned

Im vergangenen Semester fanden Veranstaltungen mit insgesamt 69 SchülerInnen an zwei allgemeinbildenden (jeweils 9. Klasse) sowie einem beruflichen Gymnasium (11. Klasse) statt. In den abschließenden Feedbackrunden sowie in einer Umfrage mittels kurzer Papierfragebögen wurde einhellig die Art der Vermittlung des Themas durch die Studierenden gelobt. Die SchülerInnen bestätigten sehr deutlich die Aussage, dass sie im Workshop viel gelernt hätten („spannend", „schockierend", „sehr überraschend", „krass" waren Adjektive, mit denen die Erfahrungen beschrieben wurden) und sie sich vornehmen, künftig mehr auf den Datenschutz zu achten. Für die Erweiterung des Konzepts und der Apps wurden hilfreiche Erkenntnisse gewonnen – so etwa hinsichtlich der im Vergleich zum Marktanteil recht geringen Verfügbarkeit von Android-Geräten unter SchülerInnen, Problemen bei der Installation der Apps sowie aufgetretenen kleineren Bugs, die es noch zu beseitigen gilt.

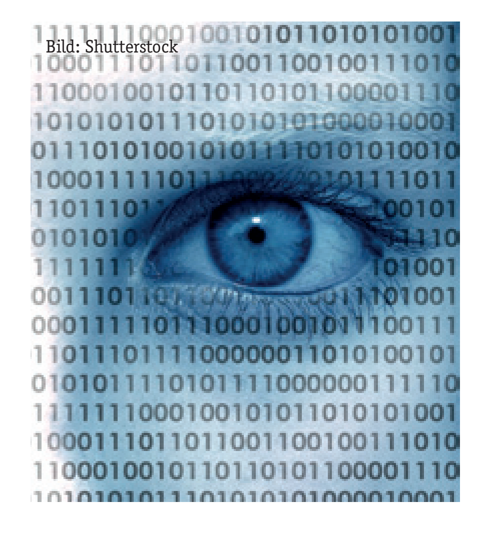
Eine Herausforderung für die Weiterentwicklung der Software besteht darin, dass sich die Studierenden jeweils nur während eines Semesters (in welchem noch weitere Lehrveranstaltungen laufen) mit dem Projekt befassen und dadurch regelmäßige Übergaben zwischen den Gruppen erforderlich sind. Doch auch die Rückmeldungen der Studierenden zeigen, dass diese sich eingehend mit Datenschutzfragen auseinandersetzen, was im Hinblick auf ihre berufliche Tätigkeit als WirtschaftsinformatikerInnen nur von Vorteil sein kann.

1 https://www.bvdnet.de/datenschutz-geht-zur-schule/

2 siehe Shortlink https://ogy.de/privacy für eine Übersicht der Projekte

3 Im Sommersemester 2019 waren an der Entwicklung und den Workshops Alexandra David, Jens Dörsam, Marian Finkbeiner, Simeon Höfer, Jan Pensel, Sarah Stadler, Maximilian Straub und Elisa Weber beteiligt.

4 https://kamba4.crux.uberspace.de


Bild: Shutterstock

Thilo Weichert

Eltern – gesetzliche Vertreter oder Dritte?

Das **Verhältnis von Eltern zu ihren Kindern** fand in der Diskussion zum Datenschutz lange Zeit keine besondere Aufmerksamkeit. Kinder tauchten im alten Bundesdatenschutzgesetz überhaupt nicht auf, wenngleich sie von Anfang an sowohl Objekt als auch Subjekt personenbezogener Datenverarbeitung waren und weiterhin sind. Was Eltern dürfen und ab wann Kindern mit und ohne ihre Eltern was erlaubt ist, wurde in der Praxis zumeist ad hoc und aus dem Bauch beantwortet. Das hat sich geändert.

Kinder stehen im besonderen Schutz der europäischen Datenschutz-Grundverordnung (DSGVO). Zugleich ergeben sich durch die extensive elterliche und frühe kindliche Mediennutzung zunehmend **informationelle Konflikte** zwischen Eltern und ihren Kindern: Diese können darauf beruhen, dass die Eltern auf Youtube peinliche Ausraster ihres Zöglings posten. Helikopter-Eltern überwachen ihre Kinder über GPS-Lokalisierung, Mikrofon und/oder Kamera von deren Smartphone. Eltern lassen Speichelproben von sich und/oder ihren Kindern genetisch untersuchen, um die biologische Vaterschaft, andere Verwandtschaftsbeziehungen oder erbliche Dispositionen zu erkunden.[1] Aber auch die Kinder können Auslöser informationeller familiärer Auseinandersetzungen sein, etwa wenn sie allzu Privates online mitteilen. Die Nutzung durch Kinder hat schon manch elterliches Endgerät zum Absturz gebracht. Besonders hart wird es nicht nur für die Teenager, sondern auch für deren Eltern, wenn ihre Kids sich als kriminelle Hacker betätigen und dabei fremde Konten plündern oder in die Privatsphäre Anderer eindringen.


Bild: ClipDealer

1. Übergeordnetes Recht

Es ist klar, dass Kinder spätestens von ihrer Geburt an im Sinne des Datenschutzes gemäß Art. 8 Grundrechte-Charta (GRCh) grundrechtsfähig sind. Ihnen steht ebenso wie allen anderen Menschen ein Grundrecht auf informationelle Selbstbestimmung zu. Damit geht aber nicht unbedingt eine eigene **Grundrechtsmündigkeit** einher. Die Grundrechtswahrnehmungs- bzw. -ausübungsfähigkeit hängt grds. von der konkreten Einsichtsfähigkeit des Kindes ab. Für diese gibt es keine starre Altersgrenze.[2] Bei grundrechtsfähigen Personen wird zunächst auch deren Ausübungsfähigkeit angenommen. Die Ausnahmen hiervon bedürfen der Begründung bzw. Rechtfertigung. Dies gilt nicht nur für den Datenschutz, sondern auch für weitere Freiheiten, insbesondere das Recht auf Meinungsäußerung und auf Information, wie es in Art. 5 Abs. 1 Grundgesetz (GG) sowie in Art. 11 GRCh gewährleistet wird, sowie für das Telekommunikationsgeheimnis nach Art. 10 GG bzw. Art. 7 GRCh. Für ihre freie Entfaltung und Entwicklung muss Kindern ermöglicht werden selbst zu bestimmen, was sie informationell tun und wie sie sich mit wem und mit welchen Inhalten austauschen.

Eine Rechtfertigung für die Einschränkung der Grundrechte der Kinder liegt im **Erziehungsrecht der Eltern**. In Art. 6 Abs. 2 GG heißt es: *Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gemeinschaft*. Dieses „natürliche Recht" dient aber nicht der Freiheitsbetätigung der Eltern. Es ist weitgehend anerkannt, dass das verfassungsrechtlich abgesicherte Sorgerecht der Eltern in erster Linie ein pflichtgebundenes und fremdnütziges Recht im Interesse des Kindeswohls ist.[3]

Die **Fremdnützigkeit** des Erziehungsrechts wird in Art. 24 GRCh unterstrichen: *(1) Kinder haben Anspruch auf den Schutz und die Fürsorge, die für ihr Wohlergehen notwendig sind. Sie können ihre Meinung frei äußern. Ihre Meinung wird in den Angelegenheiten, die sie betreffen, in einer ihrem Alter und ihrem Reifegrad entsprechenden Weise berücksichtigt. (2) Bei allen Kinder betreffenden Maßnahmen öffentlicher Stellen oder privater Einrichtungen muss das Wohl des Kindes eine vorrangige Erwägung sein. (3) Jedes Kind hat Anspruch auf regelmäßige persönliche Beziehungen und direkte Kontakte zu beiden Elternteilen, es sei denn, dies steht seinem Wohl entgegen*.

Die **kommunikative Teilhabe** der Kinder hat in der UN-Kinderrechtskonvention (UN-KRK) eine weitere übergeordnete Grundlage, wo in Art. 12 Folgendes geregelt ist: *Die Vertragsstaaten sichern dem Kind, das fähig ist, sich eine eigene Meinung zu bilden, das Recht zu, diese Meinung in allen das Kind berührenden Angelegenheiten frei zu äußern, und berücksichtigen die Meinung des Kindes angemessen und entsprechend seinem Alter und seiner Reife*. Es darf nach Art. 13 UN-KRK Medien nutzen und sich hierüber informieren: *Das Kind hat das Recht auf freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, ungeachtet der Staatsgrenzen Informationen und Gedankengut jeder Art in Wort, Schrift oder Druck, durch Kunstwerke oder andere vom Kind gewählte Mittel sich zu beschaffen, zu empfangen und weiterzugeben*. Art. 17 UN-KRK erkennt die wichtige Rolle der Massenmedien an und will sicherstellen, dass das Kind *Zugang hat zu Informationen und Material aus einer Vielfalt nationaler und internationaler*

Quellen, insbesondere derjenigen, welche die Förderung seines sozialen, seelischen und sittlichen Wohlergehens sowie seiner körperlichen und geistigen Gesundheit zum Ziel haben.

Während also das Teilhaberecht der Kinder stark ausformuliert ist, ist der Datenschutz völkerrechtlich nur über den Schutz der **Privatsphäre** abgesichert[4], z. B. in Art. 16 UN-KRK: *Kein Kind darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Das Kind hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen*. Zum Selbstbestimmungsrecht gehört es zu bestimmen, wer Zugriff auf die eigene Kommunikation erhält.

3. Zivilrecht

Das **Erziehungsrecht der Eltern** wird in § 1626 BGB einfachgesetzlich umgesetzt: *(1) Die Eltern haben die Pflicht und das Recht, für das minderjährige Kind zu sorgen (elterliche Sorge). Die elterliche Sorge umfasst die Sorge für die Person des Kindes (Personensorge) und das Vermögen des Kindes (Vermögenssorge). (2) Bei der Pflege und Erziehung berücksichtigen die Eltern die wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbständigem verantwortungsbewusstem Handeln. Sie besprechen mit dem Kind, soweit es nach dessen Entwicklungsstand angezeigt ist, Fragen der elterlichen Sorge und streben Einvernehmen an*. Damit sind Konflikte zwischen Eltern und Kinder über den Umgang mit Daten vorprogrammiert und letztlich auch mit staatlichen Einrichtungen, wenn diese sich in die informationelle Sorgebeziehung zwischen Eltern und Kindern einmischen.

Die Umsetzung der Vorgaben des übergeordneten Verfassungs- und Völkerrechts ist in einer modernen hochtechnisierten Welt nicht trivial, in der sich nicht nur der Staat, sondern auch private Dritte informationell in die Eltern-Kind-Beziehung einmischen. Kinder sind wegen ihrer Manipulierbar- und Verletzlichkeit für viele Anbieter willkommene Objekte für kommerzielle Ausbeutung.[5] Nicht zu reden von Kriminellen, die zur Befriedigung ihrer Triebe oder in der Absicht sich zu bereichern, Kindern und ihren Eltern Schaden zufügen.

Im Zivilrecht bestehen langjährig bewährte Regelungen zur Geschäftsfähigkeit von Minderjährigen. In den §§ 104 ff. BGB wird nach Fallgruppen geordnet, wann ein Kind oder ein Jugendlicher wirksam Geschäfte eingehen und abwickeln kann. Weitere **pauschalierte gesetzliche Bewertungen** finden wir im Strafrecht, also wann ein Heranwachsender für seine Taten strafrechtlich zur Verantwortung gezogen werden kann, sowie in weiteren Rechtsgebieten.[6] Mit der DSGVO haben wir nun zumindest in Bezug auf Einwilligungen bei Diensten der Informationsgesellschaft erstmals in Art. 8 DSGVO eine spezifische Regelung.

In der digitalen Welt besteht gegenüber der analogen ein praktisches Problem: Alter und schon gar nicht die „Einsichtsfähigkeit" lassen sich aus der **digitalen Distanz** direkt erkennen. Den Eltern mag es noch möglich sein den Entwicklungsstand ihrer Kinder und deren Einsichtsfähigkeit in das, was sie digital tun, einzuschätzen. Dritten, die mit ihnen nur kurz oder gar nicht direkt zu tun haben, ist dies nur schwer oder überhaupt nicht möglich.

2. Datenschutzrechtliche Willenserklärung

Bevor auf die datenschutzrechtlich relevanten Beziehungen zwischen Eltern und ihren Kindern eingegangen wird, sind einige grundsätzliche Erwägungen zu Handlungen bzw. **Erklärungen im Datenschutzrecht** nötig: Dabei wird bei Betroffenen insbesondere zwischen zwei Formen unterschieden: Einwilligung und Vertragsabschluss mit Verarbeitungsfolgen.

Von Anfang an war die rechtliche Einordnung von **Einwilligungen** im Datenschutz umstritten: Sind diese ein spezielles Rechtsgeschäft, so dass es für deren Wirksamkeit einer zivilrechtlichen Geschäftsfähigkeit bedarf?[7] Dem wurde und wird entgegen gehalten, die Einwilligung bezöge sich nicht auf ein Geschäft, sondern auf eine tatsächliche Handlung, nämlich einen Eingriff in das Persönlichkeitsrecht.[8] Als Konsequenz hieraus wurde teilweise (fälschlich) geschlossen, dass das Recht der allgemeinen Geschäftsbedingungen (AGB) auf Datenschutzeinwilligungen nicht anwendbar sei.[9] Auch die Vorschriften über die Vertretung seien nicht anwendbar; grundsätzlich müsse der Betroffene die Einwilligung selbst erteilen.[10]

Inzwischen ist weitgehend anerkannt, dass die Datenschutz-Einwilligung keine rechtsgeschäftliche Willenserklärung ist. Ähnlich wie bei medizinischen Eingriffen[11] geht es bei informationellen Maßnahmen um die Disposition über **höchstpersönliche Rechte** und Rechtsgüter. Die Einwilligung wird daher als rechtsgeschäftsähnliche Handlung oder als Realakt[12] eingestuft. Dies hat zur Folge, dass allenfalls eine analoge Anwendung der Regeln zur Geschäftsfähigkeit in Betracht kommt. Während aber bei körperlichen Eingriffen regelmäßig eine direkte Beziehung zu dem Kind besteht, über die ein Eindruck vom Kind möglich ist, fehlt bei informationellen Maßnahmen oft ein solcher Bezug. Dies ist ein Grund mehr, fixe Altersgrenzen festzulegen, so wie dies nun in Art. 8 DSGVO vorgesehen ist.

Bei informationellen Eingriffen als solche in den höchstpersönlichen Lebensbereich stellt sich die praktische Frage, ob Willenserklärungen hierzu von einem Stellvertreter abgegeben werden können. Eltern sind gemäß § 1629 Abs. 1 S. 1 BGB in rechtsgeschäftlichen Dingen **gesetzliche Vertreter** der eigenen Kinder. Die gesetzliche Vertretung beschränkt sich aber nicht auf Rechtsgeschäfte, sondern ist auch bei geschäftsähnlichen Handlungen möglich. Dies gilt z. B. für medizinische, aber auch für informationelle Maßnahmen.

Es ist streitig, inwieweit im Datenschutzrecht eine **gewillkürte Vertretung** möglich ist. So wird teilweise die Ansicht vertreten, Datenschutz-Einwilligungen seien vertretungsfeindlich.[13] Delegiert ein Betroffener seine Entscheidung über die Zulässigkeit einer Datenverarbeitung an einen Dritten, so entscheidet er nicht selbst über Verantwortlichkeit, Zweck, Art und Umfang der Datenverarbeitung. Dessen ungeachtet ist eine gewillkürte Bevollmächtigung eine spezifische Art der Wahrnehmung des eigenen Rechts auf informationelle Selbstbestimmung, wenn die Vollmach-

terteilung in informierter Weise erfolgt. Angesichts des Umstands, dass eine mit Vollmacht erteilte Einwilligung durch den Betroffenen selbst zurückgenommen werden kann, ist nicht erkennbar, weshalb dem Betroffenen diese Art der Bevollmächtigung vorenthalten werden muss.[14]

3. Gesetzliche Vertretung des Kindes

Im Hinblick auf die Vertretung der Kinder durch die Eltern spielt der Streit eine untergeordnete Rolle, da selbst die Gegner von Bevollmächtigungen die gesetzliche Vertretung im Datenschutzrecht zumeist akzeptieren.[15] Gemäß § 1629 Abs. 1 S. 1 BGB umfasst die elterliche Sorge die **gemeinschaftliche Vertretung** des Kindes, was in den Sätzen 2 und 3 präzisiert wird: *Die Eltern vertreten das Kind gemeinschaftlich; ist eine Willenserklärung gegenüber dem Kind abzugeben, so genügt die Abgabe gegenüber einem Elternteil. Ein Elternteil vertritt das Kind allein, soweit er die elterliche Sorge allein ausübt oder ihm die Entscheidung nach § 1628 übertragen ist*.

In § 1628 BGB ist vorgesehen, dass bei **Meinungsverschiedenheiten** zwischen den Eltern auf Antrag eines Elternteils das Familiengericht im Einzelfall die Entscheidung auf einen Eltenteil übertragen kann. Sind die Meinungsverschiedenheiten grundsätzlicher Art, so kann die gemeinsame Sorge gemäß § 1671 Abs. 1 S. 1 BGB vollständig aufgelöst werden: *Leben Eltern nicht nur vorübergehend getrennt und steht ihnen die elterliche Sorge gemeinsam zu, so kann jeder Elternteil beantragen, dass ihm das Familiengericht die elterliche Sorge oder einen Teil der elterlichen Sorge allein überträgt*. Gemäß Abs. 2 ist ein solcher Antrag auch möglich, wenn die Eltern nur vorübergehend getrennt leben.

Das Recht unterscheidet zwischen **Personensorge und Vermögenssorge** (§ 1626 Abs. 1 S. 2 BGB). Betreffen informationelle Maßnahmen den höchstpersönlichen Bereich des Kindes, so ist dies ein Fall der Personensorge. Gleiches gilt für Formen der Datenverarbeitung, die in einem vertraglichen Kontext stehen, ohne finanzielle Auswirkungen zu haben, so wie dies etwa bei unentgeltlicher Nutzung von Webdiensten regelmäßig der Fall ist. Ist dagegen die informationelle Maßnahme mit einer finanziellen Gegenleistung verbunden, so haben wir es mit einem Fall der Vermögenssorge zu tun. Entsprechendes kann auch ohne einen Vertrag gegeben sein, wenn mit einer informationellen Maßnahme schuldrechtliche Konsequenzen, etwa Schadensersatzansprüche, verbunden sein können. Die Grenzen sind fließend; eine Grenzziehung ist nur bei speziellen Fallkonstellationen nötig.

Neben der elterlichen Sorge gibt es weitere Formen der **per Gesetz geregelten Kindesvertretung**, die hier nur erwähnt werden können: Dies ist die Pflegschaft, bei der die Pflegeperson die Eltern in Angelegenheiten des täglichen Lebens vertritt (§ 1688 Abs. 1 BGB). Bei Maßnahmen des Jugendamtes, der Heimerziehung, der sozialpädagogischen Einzelbetreuung und der Eingliederungshilfe für seelisch behinderte Kinder und Jugendliche gilt § 1688 Abs. 2 BGB: *Der Pflegeperson steht eine Person gleich, die im Rahmen der Hilfe nach den §§ 34, 35 und 35a Abs. 1 Satz 2 Nr. 3 und 4 des Achten Buches Sozialgesetzbuch die Erziehung und Betreuung eines Kindes übernommen hat*. Im SGB VIII, das die Kinder- und Jugendhilfe regelt, sind die Pflegschaft (vgl. auch § 1909 Abs. 1 BGB) und die Vormundschaft als weitere Formen der Vertretung von Kindern geregelt (§§ 54 ff. SGB VIII), wozu auch die Amtspflegschaft und Amtsvormundschaft (§ 55 SGB VIII) gehören. Die gilt z. B. bei der Inobhutnahme von Kindern und Jugendlichen (§ 42 Abs. 3 S. 3 SGB VIII), insbesondere auch von unbegleiteten minderjährigen Flüchtlingen (§ 42a Abs. 1 SGB VIII). Die Regeln zur elterlichen Sorge sind jeweils zu übertragen.

Da die elterliche Sorge vorrangig dem Interesse des Kindes dienen soll, stellt sich die Frage, ob und inwieweit bei einer gesetzlichen Vertretung dem **Willen des Minderjährigen** entsprochen werden muss. Bei medizinischen Eingriffen ist anerkannt, dass den Minderjährigen bei schwerwiegenden Eingriffen bei ausreichender Urteilsfähigkeit ein Vetorecht zugestanden wird.[16] Dies ist auf den Datenschutz übertragbar. Eine weitergehende Form der Einbeziehung des Kindes besteht darin, kumulativ sowohl die Einwilligung des Kindes wie die der Eltern zu fordern. Dies ist insbesondere angezeigt, wenn unklar ist, ob beim Kind möglicherweise schon die für die Entscheidung nötige Einsichtsfähigkeit vorliegt. Entsprechendes gilt bei Eingriffen in die Intimsphäre sowie bei solchen, die an den Kernbereich privater Lebensgestaltung des Minderjährigen heranreichen.[17]

Bei der Bewertung des Verhältnisses zwischen Eltern und Kind ist zwischen **Innenverhältnis und Außenbeziehungen** zu unterscheiden. So kann eine elterliche Entscheidung gegenüber dem Kind eine unzulässige Beeinträchtigung sein, die aber für Dritte dennoch als wirksam angesehen werden muss, etwa weil sie nicht erkennen oder gar erkennen können, dass damit eine Kindeswohlgefährdung verbunden ist.

4. Einwilligung und Vertrag nach der DSGVO

Angesichts der obigen Erwägungen zu Kindesentwicklung und zur Einsichtsfähigkeit insbesondere im Außenverhältnis war es dem DSGVO-Gesetzgeber möglich, die Voraussetzungen für die Verarbeitung von Kinderdaten an bestimmten Altersgrenzen zu orientieren. Die DSGVO enthält aber **kein Gesamtkonzept** zum Schutz der informationellen Selbstbestimmung von Kindern.[18]

4.1. Einwilligung bei Mediendiensten

Die Regelung zur Einwilligung von Kindern in die Datenverarbeitung in Art. 8 DSGVO beschränkt sich auf die Verarbeitung bei **Diensten der Informationsgesellschaft**. Gemäß Art. 1 Abs. 1 Richtlinie (EU) 2015/1535 fällt darunter u. a. eine Dienstleistung, *die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird sowie eine auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, bei der eine Übertragung von Daten auf individuelle Anforderung erbracht wird*. Nicht erforderlich ist eine entgeltliche Leistung; es genügt, wenn die Leistung von einem Anbieter zu Werbezwecken für durch ihn verkaufte Güter oder angebotene Dienstleistungen erbracht wird.[19] Dienstleistung ist zu verstehen als selbständige Leistung im Rahmen der Dienstleistungsfreiheit, die nicht den anderen Grundfreiheiten

des AEUV (Waren-, Personen- und Kapitalverkehr) unterfällt.[20] Auf welcher vertraglichen Grundlage die Leistung erbracht wird, spielt keine Rolle.

Weitere Voraussetzung für die Anwendung des Art. 8 DSGVO ist, dass der Dienst der Informationsgesellschaft dem Minderjährigen **direkt angeboten** wird. Die Regelung des Art. 8 Abs. 1 DSGVO soll alle Dienste erfassen, die auf die Bedürfnisse von Kindern zugeschnitten sind. Erfasst sind auch solche, die zugleich auch für Erwachsene bestimmt sind.[21]

Soll eine Datenverarbeitung zu einem Kind auf Grundlage einer Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zulässig sein, so erteilt diese nach Art. 8 Abs. 1 S. 1 DSGVO vom **16. vollendeten Lebensjahr** an das Kind selbst. Gemäß Art. 8 Abs. 1 S. 3 DSGVO können *die Mitgliedstaaten durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen*. Eine solche Regelung hat Deutschland nicht erlassen.

Bei Kindern bzw. Jugendlichen unter 16 Jahren gelten die in Art. 8 Abs. 1 S. 2 DSGVO niedergelegten Grundsätze, wonach der **Träger der elterlichen Verantwortung** für das Kind oder mit dessen Zustimmung die Einwilligung erteilt.[22] Träger der elterlichen Verantwortung sind im Normalfall die Eltern, die das Kind zumeist gemeinsam nach den §§ 1626, 1626a, 1629 BGB vertreten. Ein Elternteil kann den anderen ermächtigen, die Einwilligung für das Kind zu erklären. Die Einwilligung kann durch die Eltern selbst erfolgen; möglich ist auch – soweit beim Kind die erforderliche Einsichtsfähigkeit besteht – dass das Kind das Vorliegen der Einwilligung der Eltern bestätigt.[23]

Für die **13- bis 15-jährigen** wurde in Art. 8 DSGVO keine europäische Vollharmonisierung erreicht. Auch wenn der deutsche Gesetzgeber von der spezifischen nationalen Regelungsmöglichkeit durch die Öffnungsklausel des Abs. 1 S. 3 keinen Gebrauch gemacht hat, hat dies nicht zur Folge, dass für diese Altersgruppe in Deutschland – wie vor dem Wirksamwerden der DSGVO – auf die Einsichtsfähigkeit abgestellt werden dürfte. Zweck der Regulierung war es, an die Stelle der nur im Einzelfall feststellbaren Einsichtsfähigkeit generell auf rechtssichere klare Abstufungen zu setzen.[24]

Bei **Kindern unter 13 Jahren** nimmt Art. 8 DSGVO insofern eine Vollharmonisierung vor, dass immer die Einwilligung der Eltern erforderlich ist.[25] Dahinter steht die Erwägung, dass die Kinder in diesem Alter mit den sich aus der Nutzung von Digitalgeräten möglicherweise ergebenden Problemen bei deren Eintritt nicht allein gelassen werden sollen.[26]

4.2 Einwilligung ansonsten

Da die Regelung des Art. 8 Abs. 1 DSGVO nur „in Bezug auf Dienste der Informationsgesellschaft“ anwendbar ist, stellt sich die Frage, wie bei Minderjährigen ansonsten zu verfahren ist. Diese Frage stellt sich bei Verarbeitungen von Bildern und sonstigen Daten in Sportvereinen, bei Pfadfindern oder generell bei **analogen Freizeitbetätigungen**. Art. 8 Abs. 1 DSGVO ist auch nicht anwendbar, wenn Daten und Bilder über Dienste der Informationsgesellschaft kommuniziert werden, ohne dass diese sich direkt an Kinder, vielmehr generell an die Öffentlichkeit wenden.

Da insofern in der DSGVO keine Regelung besteht, bleibt es bei der Rechtslage, die vor Wirksamwerden der DSGVO galt: Einwilligende sind einwilligungsfähig, wenn sie in der Lage sind, die Bedeutung ihrer Erklärung zu erfassen. Bei der Feststellung der **Einsichtsfähigkeit** sind Art, Umfang, Anlass und Zweck der jeweiligen Datenverarbeitung zu berücksichtigen.[27] Nach Vollendung des 16. Lebensjahrs ist generell von der Einsichtsfähigkeit auszugehen.[28]

4.3 Verträge von Minderjährigen

In Art. 8 Abs. 3 DSGVO ist geregelt, dass der Abs. 1 das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zur Rechtsverfolgung eines Vertrags in Bezug auf ein Kind, unberührt lässt. Dies betrifft auch Verträge, die Datenverarbeitung als Gegenstand haben. In diesen Fällen verweist die DSGVO auf das **nationalstaatliche Zivilrecht**, in Deutschland also auf die §§ 104 ff. BGB.

Bevor auf diese Regelungen näher eingegangen wird, muss die Frage beantwortet werden, wann ein (schuldrechtlicher) Vertrag mit Folgen für die Datenverarbeitung anzunehmen ist. Inzwischen ist allgemein anerkannt, dass auch bei einer **unentgeltlichen Inanspruchnahme von Online-Dienstleistungen** ein Vertrag Grundlage ist, wenn die Gegenleistung des Nutzenden in der Bereitstellung seiner Daten z. B. für Werbezwecke liegt. Irgendein „Entgelt“ genügt. Nach § 312 Abs. 1 BGB sind die Regelungen zur Umsetzung der Verbraucherrechterichtlinie[29] anzuwenden, wenn diese „eine entgeltliche Leistung“ zum Gegenstand haben. Werden also anstelle von Geld von einem Verbraucher Daten als Entgelt bereitgestellt, so haben wir es mit einem Verbrauchervertrag zu tun. Dies ist z. B. bei der Nutzung von sozialen Netzwerken oder Apps der Fall, deren Nutzung durch die Verbraucher die Verwendung von deren Daten für Werbezwecke bedingt.[30] Diese Sicht wird bestätigt durch die Richtlinie über vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DIRL).[31] Erfasst werden gemäß Art. 3 Abs. 1 DIRL alle Verbraucherverträge über digitale Inhalte und Dienstleistungen, für die „der Verbraucher einen Preis zahlt“, wobei dies gemäß Art. 2 Nr. 7 DIRL auch „eine digitale Darstellung eines Werts“ sein kann, die vom Verbraucher im Austausch „geschuldet wird“.[32] Die Erwägungsgründe zur DIRL stellen klar, dass die DSGVO voll zur Anwendung kommt (ErwGr. 37 DIRL). Ausschlaggebendes Merkmal für die Annahme einer Einwilligung, also nicht eines Vertrags, ist gemäß ErwGr 39 DIRL deren Widerrufbarkeit (Art. 7 Abs. 3 DSGVO).

Eine klare Abgrenzung zwischen Vertrag und Einwilligung wird auch durch Art. 7 Abs. 4 DSGVO nicht erreicht. Abgrenzungskriterium ist dabei nicht die Widerrufbarkeit, sondern schon bei der Erklärung die Freiwilligkeit. Diese soll nicht vorliegen, wenn sie für die Erfüllung des Vertrags nicht erforderlich ist. Die Regelung wird als **Koppelungsverbot** bezeichnet: Es soll unzulässig sein, eine für die Vertragserfüllung nicht nötige Einwilligung mit einem Vertragsabschluss zu koppeln. Der Vertragsinhalt und damit, was für die Vertragsabwicklung „erforderlich“ ist, wird regelmäßig nicht vom Verbraucher, sondern vom Unternehmen festgelegt. Gerade wenn

Daten als Gegenleistung eingefordert werden, lässt sich deren „Erforderlichkeit" nicht nach klaren Kriterien überprüfen. Letztlich läuft die Regelung darauf hinaus, dass die Aufsichtsbehörden und Gerichte die Abgrenzung vornehmen müssen, indem sie bestimmte Koppelungen als treuwidrig oder Verstoß gegen die guten Sitten beanstanden.[33]

Aus dem oben Gesagten ergibt sich, dass ein Vertrag i. S. v. Art. 6 Abs. 1 lit. c DSGVO mit einem Minderjährigen (über die Nutzung eines Dienstes der Informationsgesellschaft) zustande kommt, wenn der Minderjährige keine Möglichkeit hat, der Nutzung seiner Daten, die nicht für die Erbringung des Dienstes erforderlich sind, zu widersprechen. Die **Wirksamkeit des Vertrages** richtet sich dann gemäß Art. 8 Abs. 3 DSGVO nach den §§ 104 ff. BGB. Unwirksam gemäß den rechtsgeschäftlichen Regeln sind danach Verträge mit Kindern unter sieben Jahren (§§ 104 Nr. 1, 105 Abs. 1 BGB). Minderjährige zwischen dem 7. und dem 18. Lebensjahr sind beschränkt geschäftsfähig (§ 106 BGB). Verträge sind in dieser Altersspanne wirksam, wenn sie für den Minderjährigen lediglich einen rechtlichen Vorteil erbringen oder der gesetzliche Vertreter zugestimmt hat oder die „vertragsmäßige Leistung mit Mitteln bewirkt" wird, die dem Minderjährigen „zu diesem Zwecke oder zur freien Verfügung" überlassen worden sind (Taschengeldparagraf) (§§ 107-110 BGB).

4.4 Die Rolle der Eltern

Die Eltern sind also weiterhin nach den aktuell geltenden Regelungen bis zum 16. oder gar bis zum 18. Lebensjahr wichtig. Ob und was sie erlauben, ist für die Datenverarbeitung zu ihren Kindern zumindest bei bedeutenden Vorgängen bestimmend. Wie starr die Vorgaben gehandhabt werden, hängt vom **pädagogischen** Konzept der Eltern ab. Dieses soll sich natürlich am Kindeswohl ausrichten. Um altersgemäß vorzugehen, bietet es sich in der Praxis an, dass sie ihre Zustimmung im frühen Kindesalter jeweils in Einzelgenehmigungen erteilen und im höheren Alter pauschalere und inhaltlich weitergehende Erlaubnisse erteilen.[34] Die Zustimmung kann dem Datenverarbeiter oder dem eigenen Kind erteilt werden.[35] Beschränkungen können die Eltern auch mit Hilfe von technischen Mitteln realisieren.

Angesichts der oben dargestellten komplizierten Rechtslage dürften Eltern oft überfordert sein bei der Frage, ob ihre Kinder eine Datenverarbeitung über sich legitimieren dürfen oder ob sie als Erziehungsberechtigte hierbei (zwingend) gefordert sind. Als Richtschnur kann gelten, dass die Selbstbestimmung der Kinder unter 13 Jahren praktisch in jedem Fall von der Zustimmung der Eltern abhängig gemacht werden kann. Bei Heranwachsenden zwischen 16 und 18 Jahren bestehen dagegen nur sehr eingeschränkte Interventionsmöglichkeiten. Zwischen 13 und 15 Jahren haben die Eltern Einflussmöglichkeiten. Letztlich läuft es – trotz aller Pauschalierungsbemühungen des Gesetzgebers für die Dienstebetreiber – darauf hinaus, dass die Eltern auf die Einsichtsfähigkeit abstellen müssen. Je älter und einsichtiger die Heranwachsenden werden, umso mehr Selbstbestimmungsmöglichkeiten sind ihnen einzuräumen. Zwar sieht die DSGVO nicht das Erfordernis einer doppelten Einwilligung von Eltern und Kind vor, doch sollten alle Beteiligten einen Konsens anstreben (Double-Opt-in-Verfahren).[36] Mit der „Zustimmung" des Kindes sind die Eltern auf der sicheren Seite (Art. 8 Abs. 1 S. 2 letzte Alt. DSGVO).[37]

5. Verarbeitung ohne und gegen den Kindeswillen

Die **Unart vieler Eltern** ohne und gegen den Willen ihrer Kinder Daten über diese im Internet zu veröffentlichen, führt zu der Frage, ob bzw. inwieweit dies überhaupt zulässig ist. Das scheinbar unreflektierte Posting von Baby- und Kinderfotos oder -videos stößt auf Kritik und führt zu rechtlichen Überlegungen. Hoch umstritten – pädagogisch wie rechtlich – sind auch Überwachungsmaßnahmen der Eltern, mit denen diese für ihre Kinder mehr Sicherheit gewährleisten wollen.

Bei solchen Aktivitäten handeln die Eltern als Verantwortliche.[38] Wegen der eigenständigen Grundrechtsfähigkeit ihrer Kinder sind diese von einer **Datenverarbeitung** durch dritte Verantwortliche „Betroffene". Es verbietet sich insofern Eltern und Kinder als rechtliche Einheit zu behandeln. Dies hat zur Folge, dass es für die Verarbeitung der Kindesdaten einer rechtlichen Legitimation gemäß Art. 6 DSGVO bedarf.[39]

Etwas anderes gilt freilich, wenn die Eltern für ihr **Kind in dessen Namen** tätig werden. Dies gilt z. B. für eine Einzahlung von Erspartem auf ein Bankkonto des Kindes. Ein Minderjähriger kann auch als Verantwortlicher für eine Webseite handeln. Nehmen Eltern hierbei für ihren Nachwuchs Änderungen vor, so ist dies keine Drittdatenverarbeitung. Voraussetzung ist aber, dass der Heranwachsende hiervon zumindest Kenntnis hat.

Im engsten Familienkreis besteht ein ehrschutzfreier Raum.[40] Dies bedeutet, dass Persönlichkeitsverletzungen innerhalb dieses Kreises nur in besonderen Ausnahmefällen rechtlich geltend gemacht werden können. Dies findet auch seinen Ausdruck in der **Haushaltsausnahme** des Art. 2 Abs. 2 lit. c DSGVO. Die DSGVO ist demnach bei der „Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" nicht anzuwenden. Etwas anderes gilt, wenn eine Datenverarbeitung über den familiären Bereich hinausreicht. Dies ist der Fall bei Baby- und Kinderfotos im Internet.[41] Es ist auch der Fall beim Einsatz von Überwachungssoftware, bei der Datenübermittlungen an den Dienstleister und oft an weitere Stellen erfolgen.[42]

Als Legitimation kommt zunächst die **Einwilligung** in Betracht (Art. 6 Abs. 1 lit. a DSGVO). Die können sich die Eltern bei ihren Kindern einholen. Fragwürdig dürfte in der Praxis dabei oft die Freiwilligkeit sein. Dann stellt sich die Frage der Einsichtsfähigkeit. Fehlt die, so könnten die Eltern als gesetzliche Vertreter ihrer Kinder handeln, also sich selbst eine Einwilligung zur Verarbeitung erteilen. Dies ist aber ein sog. Insichgeschäft, das gemäß § 181 BGB verboten ist: *Ein Vertreter kann, soweit nicht ein anderes ihm gestattet ist, im Namen des Vertretenen mit sich im eigenen Namen oder als Vertreter eines Dritten ein Rechtsgeschäft nicht vornehmen, es sei denn, dass das Rechtsgeschäft ausschließlich in der Erfüllung einer Verbindlichkeit besteht.* Auch wenn die Regelung auf Rechtsgeschäfte beschränkt ist, ist die zugrunde liegende Erwägung auf die Datenverar-

beitung übertragbar, was eine Einwilligung der Eltern für eine eigene Nutzung verbietet.[43]

In Frage kommt eine Legitimation der Verarbeitung von Kindesdaten durch die Eltern nach Art. 6 Abs. 1 lit. c oder lit. e DSGVO. Es kann aber nur selten angenommen werden, dass die Verarbeitung „zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich ist". Derartige Verpflichtungen lassen sich annehmen bei rechtlich geforderten Übermittlungen in bestimmten Lebenssituationen, etwa dem Vorzeigen des Ausweises bei einem Grenzübertritt oder bei Angaben zum Kind in einer Steuererklärung. Es besteht aber keine Verpflichtung zur Online-Präsentation eines Kindes; auch die technische Überwachung des eigenen Kindes dürfte nur in sehr spezifischen Risikosituationen zur rechtlichen Pflicht gerinnen.

Näher liegend ist es, bestimmte Formen der Verarbeitung als eine Aufgabenwahrnehmung **„im öffentlichen Interesse"** einzustufen. Es ist unbestreitbar, dass das Wahrnehmen der elterlichen Sorge nach § 1626 BGB im „öffentlichen Interesse" liegt (lit. e). Da in lit. e Hoheitsträger sich i. d. R. auf die 2. Alternative „Ausübung öffentlicher Gewalt" berufen können, gilt die 1. Alternative vor allem für Private, wozu auch Eltern in ihrer sorgenden Funktion zählen. Um einen informationellen Eingriff legitimieren zu können, muss das jeweilige öffentliche Interesse ein solches Gewicht haben, dass die Maßnahme verhältnismäßig ist.[44] Sie muss sich auf das absolut Notwendige beschränken.[45] Das Veröffentlichen von Kinderbildern kann hierüber definitiv nicht gerechtfertigt werden; bei technischer Kinderüberwachung kommt es – abhängig von der Gefahrenlage – auf das Ergebnis der Verhältnismäßigkeitsprüfung an. Da regelmäßig weniger überwachungsintensive Alternativmaßnahmen zur Gewährleistung der Sicherheit der Kinder möglich sind, dürfte diese Regelungsalternative eine Verarbeitung nur selten rechtfertigen.

Schließlich ist eine Verarbeitung erlaubt zur **Wahrung berechtigter Interessen**, sofern nicht Schutzinteressen des Kindes überwiegen (Art. 6 Abs. 1 lit. f DSGVO). Die Regelung erwähnt den Kindesschutz ausdrücklich. Meinungsäußerungen erfolgen i. d. R. in Wahrnehmung eines berechtigten Interesses. Auch die öffentliche Selbstdarstellung ist ein berechtigtes Interesse. Diese darf sich aber nicht zulasten des Kindes auswirken. Die Dokumentation eines öffentlichen Ereignisses ist eher berechtigt als die Darstellung eines privaten Vorgangs. Eine Online-Bereitstellung von Kindesbildern kann nur als zulässig angesehen werden, wenn adäquate Schutzmaßnahmen ergriffen werden. Diese können in einer Zugriffsbeschränkung auf eine Nutzergruppe bestehen. Mit einer Verpixelung von Gesichtern oder anderen Anonymisierungsmaßnahmen kann eine Identifizierung erschwert oder verhindert werden.[46]

Die **Wahrnehmung der elterlichen Sorge** nach § 1626 BGB ist nicht nur eine öffentliche Aufgabe, sondern auch ein berechtigtes Interesse der Eltern. Bei der Erforderlichkeitsprüfung nach lit. f muss ein weniger strenger Maßstab als bei lit. e angelegt werden. Wegen der Kindeswohlorientierung ist aber das Kind vor der jeweiligen Maßnahme einzubeziehen.[47] Zudem ist darauf zu achten, dass keine sensitiven Daten, etwa zur Gesundheit erfasst werden, da insofern ein zusätzlicher Legitimationsbedarf gemäß Art. 9 Abs. 2 DSGVO besteht.[48] Auch das Tracking, bei dem Bewegungsprofile entstehen, ist als besonders sensitiv anzusehen (vgl. § 98 TKG).[49]

Die elterliche Kindesüberwachung wird problematischer, wenn auch die **Daten Dritter** erfasst werden. Das Recht zur elterlichen Sorge legitimiert i. d. R. nur die Verarbeitung der Daten des Kindes. Die Daten Dritter werden aber oft miterfasst, etwa zwangsläufig bei einer akustischen oder optischen Kontrolle. Ohne eine angemessene Berücksichtigung von deren schutzwürdigen Interessen geht es nicht. Lässt sich diese nicht umsetzen, so ist die Überwachungsmethode unzulässig.

In diesem Zusammenhang soll kurz auf die Frage eingegangen werden, inwieweit die seit 1907 geltenden Regelungen des Kunsturhebergesetzes (KUG) mit dem Wirksamwerden der DSGVO weitergelten. Diese machen Aussagen zur **Veröffentlichung von Bildern** – auch von Kindern – und setzen bei einer Identifizierbarkeit regelmäßig die Zustimmung des Betroffenen voraus. Da das KUG schematische Vorgaben macht und keine Abwägung vorsieht, muss das KUG, trotz der Öffnungsklausel in Art. 85 DSGVO als obsolet angesehen werden. Die dort genannten Regelbeispiele können aber als Abwägungskriterien nach Art. 6 Abs. 1 lit. f DSGVO Berücksichtigung finden.[50]

Ein Spezialfall, bei dem die Daten Dritter mit erfasst werden, ist die Kontrolle der **Telekommunikation des Kindes**. Hier steht nicht nur der Datenschutz, sondern auch das Telekommunikationsgeheimnis (Art. 10 GG, Art. 7 GRCh, § 88 TKG) auf dem Spiel, das nicht nur das Kind, sondern auch dessen Kommunikationspartner schützt. Der Schutz beschränkt sich aber auf die Informationsübermittlung. Er endet, wenn eine Nachricht beim Empfänger angekommen ist und von diesem abgerufen wurde, so dass er diese zur Kenntnis nehmen und evtl. weiterverarbeiten konnte.[51] Wurde also eine Kommunikation vom Kind abgerufen und auf seinem Mobilgerät dargestellt, stehen die dabei erlangten Daten in der zunächst unbeschränkten Verfügungsmacht des Kindes. Greifen die Eltern hierauf zu, so ist das Kommunikationsgeheimnis nicht mehr tangiert. Dies gilt auch im Hinblick auf die Absender der Kommunikation. Der Absender einer Nachricht kann zwar darauf vertrauen, dass ein Telekommunikations-Diensteanbieter die Nachricht nur für das Empfängerkonto zur Verfügung stellt. Es besteht aber kein schutzwürdiges Vertrauen darauf, dass danach nur der Kontoinhaber und nicht Dritte von dem Kontoinhalt Kenntnis erlangen. Er muss damit rechnen, dass der Empfänger Dritten Zugang gewährt.[52] Der Schutz der Daten der Kommunikationspartner des Kindes beschränkt sich darauf, dass deren Interessen im Rahmen einer Abwägung nach Art. 6 Abs. 1 lit. f DSGVO gewahrt werden müssen.

6. Schlussfolgerungen

Dadurch, dass die DSGVO den Datenschutz von Kindern besonders betont, ist noch nicht viel gewonnen. Die Regelungsstruktur ist verwirrend, für juristisch nicht geschulte Eltern undurchsichtig. Große Unsicherheit besteht,

ob und unter welchen Voraussetzungen Eltern für ihre Kinder über eine Datenverarbeitung bestimmen können. Die hierzu vorliegenden Meinungen in der Datenschutzliteratur und in der Rechtsprechung liefern kein klares Bild. Die elterliche Sorge stellt unzweifelhaft ein berechtigtes Interesse dar; ebenso unzweifelhaft ist aber, dass auch die Eltern das Recht ihrer Kinder auf informationelle Selbstbestimmung sowie sonstige Grundrechte beachten müssen. Bisher ist das Thema der Datenverarbeitung zu Kindern ein Thema für Untergerichte, wobei deren datenschutzrechtliche Weisheit manchmal eher begrenzt ist. Es wäre daher wünschenswert, wenn es wegen zentraler Grundsatzfragen zur Vorlage beim Europäischen Gerichtshof kommen würde, der europaweit verbindliche Vorgaben machen kann. Eines ist jedenfalls klar: Angesichts der Digitalisierung des Lebens von Kindern und Jugendlichen gewinnen damit verbundene Rechtsfragen zunehmend an Bedeutung.

1 Weichert, DANA 3/2019, 142; Weichert, DuD 2018, 150.

2 Spickhoff, FamRZ 2018, 412 f.; Möhrke-Sobolewski/Klas, K&R 2016, 373 f.

3 BVerfG 29.07.1968 – 1 BvL 20/63, 1 BvL 31/66, 1 BvL 5/67, Rn. 43, 60 (3. LS), NJW 1968, 2233 = FamRZ 1968, 578, Spickhoff, FamRZ 2018, 419.

4 Allgemein siehe z. B. Weichert, DuD 2014, 402 ff.

5 Möhrke-Sobolewski/Klas, K&R 2016, 373.

6 Siehe den Überblick bei Möhrke-Sobolewski/Klas, K&R 2016, 376.

7 So z. B. Kilian/Heussen-Weichert, Computerrechts-Handbuch, Stand Mai 1993, Kap. 132 Rn. 154.

8 So z. B. Ordemann/Schomerus/Gola, BDSG, 5. Aufl. 1992, § 4 Anm. 5.3; schon Auernhammer, BDSG, 1977, § 3 Rn. 7.

9 So z. B. Schütte, NJW 1979, 592 f.; zur heutigen Rechtslage Ernst, DANA 2017, 15.

10 So Auernhammer, Bundesdatenschutzgesetz, 3. Aufl. 1993, § 4 Rn. 11.

11 Spickhoff, FamRZ 2018, 416.

12 Gola-Schultz, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 8; zur urheberrechtlichen Einwilligung BGH 19.10.2011 – I ZR 140/10, Rn. 18, 25, 27, vgl. Ernst DANA 2017, 14.

13 Simitis/Hornung/Spiecker-Klement, Datenschutzrecht, 2019, Art. 7 Rn. 37; Ernst, ZD 2017, 111; Simitis-Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014, § 4a Rn. 39 f.: Bevollmächtigter ist allenfalls „Bote“.

14 So Kühling/Buchner-Buchner/Kühling, DS-GVO BDSG, 2. Aufl. 2018, Art. 7 Rn. 31; Gola/Schomerus, BDSG, 12. Aufl. 2015, § 4a Rn. 25.

15 Simitis/Hornung/Spiecker-Klement (En. 13), Art. 7 Rn. 37, Art. 8 Rn. 25; zur Vertretung im Betreuungsverhältnis AG Gießen 16.07.2018 – 230 XVII 381/17 G.

16 Buchner, FamRZ 2019, 668; BGH 10.10.2006 – VI ZR 74/05, 1. LS, Rn. 17; NJW 2007, 217 = FamRZ 2007, 130; Spickhoff, FamRZ 2018, 421.

17 Spickhoff, FamRZ 2018, 422 f.

18 Häring/Nohr, DANA 4/2018, 186; Däubler/Wedde/Weichert/Sommer-Däubler, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 8 Rn. 3.

19 EuGH 15.09.2016 – C-484/14.

20 Kühling Buchner-Schröder (En. 14), Art. 4 Nr. 26 Rn. 8.

21 Däubler/Wedde/Weichert/Sommer-Däubler (En. 18), Art. 8 Rn. 5; Kühling/Buchner-Buchner/Kühling (En. 14), Art. 8 Rn. 15 f.; Paal/Pauly-Frenzel, DS-GVO BDSG, 2. Aufl. 2018, Art. 8 Rn. 7; Ehmann/Selmayr-Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 8 Rn. 20; Sydow-Kampert, Europäische Datenschutzgrundverordnung, 2017, Art. 8 Rn. 9.

22 Diese Grenze wird von vielen als nicht mehr zeitgemäß angesehen, vgl. Häring/Nohr, DANA 2018, 186.

23 Däubler/Wedde/Weichert/Sommer-Däubler (En. 18), Art. 8 Rn. 8 f.; Kühling/Buchner-Buchner/Kühling (En. 14), Art. 8 Rn. 20.

24 Kühling/Buchner-Buchner/Kühling (En. 14), Art. 8 Rn. 3, 22; a. A. wohl Paal/Pauly-Frenzel (En. 21), Art. 8 Rn. 18.

25 Kühling/Buchner-Buchner/Kühling (En. 14), Art. 8 Rn. 22.

26 AG Bad Hersfeld 15.05.2017 – F 120/17 EASO, S. 21.

27 Simitis/Hornung/Spiecker-Klement (En. 13), Art. 8 Rn. 10.

28 Simitis/Hornung/Spiecker-Klement (En. 13), Art. 8 Rn. 12.

29 VRRL, Richtlinie 2011/83/EU v. 25.10.2011, ABl. L 304 v. 22.11.2011, S. 64.

30 Halm, DANA 2017, 12 f.

31 DIRL, Richtlinie (EU) 2019/770 v. 20.05.2019, ABl. L 136/1 v. 22.05.2019, umzusetzen bis zum 01.07.2021.

32 Halm, DANA 2017, 11.

33 Engeler, ZD 2018, 60.

34 Für die Zulassung einer pauschalierten Vorsorgevollmacht zur Datenverarbeitung Buchner, FamRZ 2019, 670.

35 Simitis/Hornung/Spiecker-Klement (En. 13), Art. 8 Rn. 26.

36 Möhrke-Sobolewski/Klas, K&R 2016, 377 f.

37 Buchner, FamRZ 2019, 668.

38 Buchner, FamRZ 2019, 666 f.

39 Buchner, FamRZ 2019, 669.

40 OLG Frankfurt 17.01.2019 – 16 W 54/18, AfP 2018, 166.

41 Buchner, FamRZ 2019, 666.

42 Buchner, FamRZ 2019, 667 f.

43 Buchner, FamRZ 2019, 667.

44 Simitis/Hornung/Spiecker-Roßnagel (En. 13), Art. 6 Abs. 1 Rn. 71; zum Verhältnis Betreuer-Betreuter Buchner, FamRZ 2019, 669.

45 Simitis/Hornung/Spiecker-Roßnagel (En. 13), Art. 6 Abs. 1 Rn. 77; EuGH 16.12.2008 – C-73/07 Rn. 56; EuGH 21.12.2016 – C-203/15 u. c-698/15, Rn. 96.

46 Buchner, FamRZ 2019, 667.

47 Buchner, FamRZ 2019, 668.

48 Buchner, FamRZ 2019, 669.

49 Weichert, Geomarketing und Datenschutz, in: LDI NRW, Living by Numbers, 2005, 135 ff.; Buchner, FamRZ 2019, 668.

50 Benedikt/Kranig, ZD 2019, 6.

51 BVerfG 13.11.2010 – 2 BvR 1124/10, Rn. 13, WM 2011, 211 = K&R 2011, 320; mit Verweis auf BVerfG 02.03.2006 – 2 BvR 2099/04, Rn-. 72 f., BVerfGE 115, 166 = NJW 2006, 976; ebenso BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 185.

52 BGH 12.07.2018 – III ZR 183/17 Rn. 73, NJW 2018, 3178 = DuD 2018, 647; Buchner, FamRZ 2019, 670.

Susanne Holzgraefe

Fotos von Kindern und Jugendlichen


Bild: ClipDealer

Vorwort

Fotos von Kindern und Jugendlichen sind nicht nur in Kindergärten, Kindertagesstätten und Schulen ein Thema, sondern auch in vielen Vereinen. Spenden lassen sich besser sammeln, wenn Fotos von Kindern gezeigt werden. Es ist ja auch nicht verboten, mit Kinderfotos Werbung zu machen. Es müssen lediglich alle Gesetze und Vorschriften zur Wahrung der Persönlichkeitsrechte der abgelichteten Kinder eingehalten werden. Das bedeutet, für alle identifizierbaren Kinder bedarf es einer rechtsgültigen Einwilligung aller Erziehungsberechtigten, dass das Abbild des Kindes für die entsprechende Werbeaktion mit Angabe der Dauer der Werbung verwendet werden darf. Die Dauer spielt hier eine nicht unerhebliche Relevanz. Wohl kaum ein Kind möchte auch nach fünfzig Jahren noch immer sein Gesicht auf der Schokoladenverpackung im Handel sehen. Das ist nicht neu, sondern galt auch schon nach altem Recht.

In vielen Einrichtungen herrscht eine große Unsicherheit, was das Thema Fotos angeht. „Dürfen wir Fotos von den Kindern in der Gruppe im Gruppenraum aufhängen?" „Dürfen wir Fotos von den Kindern im Klassenzimmer aufhängen?" „Dürfen wir Fotos von Schülern in der Aula aufhängen?" „Dürfen wir den Eltern eine Mappe mit Fotos von der Veranstaltung mitgeben?" „Dürfen die Besucher Fotos von der Bühnen-Aufführung der Kinder machen?" „Darf ich noch die Babyfotos meiner Patientinnen in meiner Praxis aufhängen." „Warum dürfen wir denn die Kinderfotos aus Afrika auch nur unter Berücksichtigung aller europäischen Gesetze und Vorschriften veröffentlichen?" „Was ist mit Gruppenfotos?" „Ab wie viel Kindern auf einem Bild brauche ich keine Einwilligung?" „Dürfen Fotos von Veranstaltungen im Kindergarten oder der Schule gemacht werden?" „Wie sollen wir denn verhindern, dass die Kinder selbst Fotos machen und ins Netz posten?" „Wir können doch nichts dafür, wenn die Oma die Fotos, die sie während der Schulveranstaltung gemacht hat, ins Netz stellt." „Mitgliederversammlungen sind doch private Veranstaltungen, da dürfen wir doch Kinderfotos zeigen, oder?" Fragen über Fragen.

Fotos und Bilder bestimmen unseren Alltag. Ein Bild sagt mehr als tausend Worte. Und genau da liegt die Gefahr. Wer kennt sie nicht, die Fotos aus Kindertagen, die besser tief im Schrank vergraben im Fotoalbum der Familie vergessen werden. Die Gesetze und Vorschriften rund um den Datenschutz gelten natürlich auch, wenn die Kinder nicht aus der EU kommen, die Bilder aber im Geltungsbereich der entsprechenden Gesetze und Vorschriften verteilt oder veröffentlicht werden. Die Datenschutzgrundverordnung (DSGVO) ist für alle Kinderfotos zu beachten, mit denen innerhalb der EU geworben oder berichtet wird, egal ob das Kind aus Afrika, der Schweiz oder dem Weltraum stammt.

Gewalt am Kind

Es gibt Vertretende, die die ungenehmigte Verteilung oder Veröffentlichung von Kinderfotos als Gewalt am Kind sehen. Nein bleibt Nein. Wenn das Kind nicht fotografiert werden möchte, dann spielt das Alter des Kindes keine Rolle. Wenn das Kind „Nein" sagt, dann darf kein Foto vom Kind gemacht werden. Für ein Kinderfoto müssen alle Erziehungsberechtigten und das Kind „Ja" sagen. Die DSGVO erlaubt zwar, dass Kinder ab einem Alter von sechzehn auch ohne Einwilligung der Eltern Diensten der Informationsgesellschaft, wie Online Spielen oder Sozialen Medien, zustimmen dürfen, aber hier ist dennoch das Erziehungsrecht zu beachten und genaustens zu prüfen, welche Art von Informationen Jugendliche hier preisgeben sollen.

Bei Aktfotos von Sechzehn- oder Siebzehnjährigen ist es ratsam, wenn die Fotografen immer die Genehmigung aller Erziehungsberechtigten einholen, auch wenn das gegebenenfalls nicht von den Gesetzgebenden vorgesehen ist und die Aufnahme rein künstlerische Zwecke verfolgt. Eltern und auch Lehrende sollten junge Menschen frühzeitig darüber aufklären, dass das Aktfoto als Geburtstagsgeschenk für den Freund keine gute Idee ist, da die

Gefahr, dass es sehr schnell im Internet landet, sehr hoch ist.

Eltern und Erziehungsberechtigte sollten sich wohl überlegen, wann sie zustimmen. Sie sollten auch darüber nachdenken, was passiert, wenn das Kind volljährig ist und so gar nicht mit der Veröffentlichung des Fotos einverstanden war. Wenn das erwachsene Kind unter der Veröffentlichung leidet. Wenn dem Kind durch die Veröffentlichung des Fotos ein Schaden entstanden ist. Zum Beispiel, weil die Person durch ein misszuverstehendes Foto den Job nicht bekommen hat oder das Kind wegen eines veröffentlichten Fotos gemobbt wurde. Könnte das erwachsene Kind hier Schadensersatz von den Eltern fordern? Haben die Eltern durch die Zustimmung psychische Gewalt am Kind zugelassen?

Fotografieren verboten

Werden Fotos im Kindergarten oder in der Schule aufgenommen, so ist die Schule oder der Kindergarten für die Fotos verantwortlich. Egal ob die Betreuenden oder Eltern oder andere Besucher die Fotos geschossen haben. Tauchen Fotos aus der Einrichtung in der Presse oder in sozialen Medien auf, ohne dass die Einrichtung eine schriftliche Einwilligung aller Erziehungsberechtigten nachweisen kann, kann es für die Einrichtung erhebliche Probleme geben. Das gilt auch, wenn Fotos über den Zaun hinweg von spielenden Kindern auf dem Spielplatz der Einrichtung an die Öffentlichkeit geraten.

Daher sind Kindergärten, Schulen und andere Betreuungseinrichtungen gut beraten, wenn sie das Fotografieren auf ihrem Gelände verbieten. Eine durchgestrichene Kamera sichtbar an den Zäunen und im Eingangsbereich der Einrichtung aufgehängt, sollte hinreichend eindeutig sein. Den Eltern zusätzlich mit den Unterlagen zur Anmeldung schriftlich den Hinweis mitzugeben, dass auf dem gesamten Gelände Fotografieren, Filmen und Tonaufnahmen verboten sind, ist förderlich. Ratsam ist auch, dass bei Veranstaltungen alle Besuchenden noch einmal explizit auf das Verbot aufmerksam gemacht werden. Das kann zum Beispiel während der Begrüßungsrede sein oder bei der Einlasskontrolle. Auf diese Weise hat die Einrichtung die Chance den Schaden nicht allein zu tragen, wenn Eltern oder Großeltern trotzdem heimlich Bilder von den Kindern beim Krippenspiel machen und veröffentlichen.

„Wir wollen aber doch Erinnerungsfotos unserer Kinder" kommt häufig als Gegenwind von Eltern und anderen Verwandten, wenn sie mit der Tatsache des Fotoverbotes konfrontiert werden. Vor allem, wenn die Kinder ein Theater- oder Musikstück aufführen. Das ist natürlich kein Problem, denn selbstverständlich kann die Einrichtung professionelle Fotografen und auch die Presse akkreditieren, Fotos unter Einhaltung der datenschutzrechtlichen Bestimmungen aufzunehmen und zu veröffentlichen oder auch Fotos einzelner Kinder für das private Fotoalbum zu machen, die die Eltern dann (gegen Entgelt) erwerben können. Sobald die Kinder identifizierbar sind, also ihre Identität durch automatische Scanner feststellbar ist, ist aber dennoch eine Einwilligung aller abgelichteten Kinder sowie derer Erziehungsberechtigten erforderlich.

Sollen die Fotos nur für das heimische Fotoalbum verteilt werden, so ist es zwingend erforderlich, dass die Nutzungsbedingungen klar und eindeutig dem Foto bei der Aushändigung mitgegeben werden. Bei Papierfotos ist es ratsam, sie auf die Rückseite zu schreiben. Bei Jahres- und Erinnerungsbüchern ist es ratsam eine Seite am Anfang den Nutzungsbedingungen zu widmen.

Nutzungsbedingungen

Dass Eltern und andere Verwandte gerne ein paar Erinnerungsfotos der Kinder haben möchten, ist verständlich. Egal ob vom Krippenspiel, der Einschulung, der Kindergarten-Abschiedsfahrt, der Konfirmation oder der Theateraufführung. Es gibt viele Ereignisse, die seit Generationen mit Fotos festgehalten und Jahre später in Fotoalben wiederentdeckt werden.

Fotos, die rein für den privaten Gebrauch gedacht sind und auf denen nicht nur die eigenen Kinder sondern auch andere Kinder identifizierbar abgelichtet wurden, dürfen ohne Einverständnis der anderen Kinder und deren Erziehungsberechtigten nicht weitergegeben, kopiert oder veröffentlicht werden. Veröffentlichen bedeutet auch, in den sozialen Netzen teilen. Hier ist auch darauf zu achten, dass digitale Fotos nicht in unsicheren Clouds von Drittanbietern oder auf unsicheren Servern landen.

Das Risiko, dass Fotos, die nur zum rein privaten Gebrauch aufgenommen und an die Kinder beziehungsweise deren Eltern verteilt wurden, doch (versehentlich) veröffentlicht oder an unbefugte Dritte weitergeleitet werden, ist extrem hoch, wenn die Fotos digital verteilt werden. Natürlich besteht auch ein Risiko, wenn die Fotos auf Papier verteilt werden, aber die Hürde ist höher. Daher ist es ratsam, wenn Erinnerungsfotos für den privaten Gebrauch angefertigt werden, auf denen nicht nur das eigene Kind abgelichtet ist, sie ausschließlich auf Papier zu verteilen und das Einscannen, was ja eine Form der Vervielfältigung ist, zu verbieten.

Einwilligung

Bevor ein Kind identifizierbar fotografiert wird, bedarf es der Einwilligung des Kindes und aller Erziehungsberechtigten. Werden nicht alle Erziehungsberechtigten gefragt, kann ein Kindergarten oder auch eine Schule schnell zum Spielball im Scheidungskrieg werden. Ein Elternteil hat zugestimmt, der andere wurde nicht gefragt und klagt jetzt, dass das Kind ohne sein Einverständnis fotografiert wurde. Daher sollten Einrichtungen wie Schulen und Kindergärten stets die Einwilligung Aller einholen. Identifizierbar heißt, dass das Kind durch automatische Bildscanner identifiziert werden kann.

Eine Einwilligung muss zweckgebunden sein. Der Zweck muss genausten beschrieben sein. Das heißt, es muss auf der Einwilligung klar und deutlich dargestellt werden, was mit den Aufnahmen passiert, wann und wo genau sie veröffentlicht werden. Es ist zu empfehlen Kästchen zum Ankreuzen zu verwenden. Zum Beispiel: für die Verteilung zum privaten Gebrauch an alle Eltern der Gruppe, zum Aufhängen im Gruppenraum, zum Aufhängen in der Aula, für die lokale Presse, für Flyer, für Soziale Medien und so weiter. Die Kästchen dürfen nicht vorausgewählt werden. Soziale Medien sollten eventuell genauer spezifiziert werden.

Zum Beispiel: Veröffentlichung auf dem YouTube-Kanal des Kindergartens, bei Facebook, im Dropbox-Portal des Kindergartens oder bei Weibo.

Auch darf die Einwilligung keine Vorteile bringen. Eine Nicht-Einwilligung darf nicht zu Nachteilen führen, denn sonst ist die Freiwilligkeit der Einwilligung nicht sichergestellt.

Wichtig ist auch, die Dauer der Verwendung in der Einwilligung festzulegen. Zum Beispiel: „Der Flyer wird ein Jahr lang verteilt.", „Die Fotos bleiben ein Jahr auf unserer Webseite.", „Für den Zeitungsbericht am 25.7.2020 zum Tag der offenen Kindergarten-Tür.", „Der Beitrag im YouTube-Kanal wird nach einem Jahr gelöscht." oder „Die Fotos liegen drei Monate in der Dropbox, dann werden sie gelöscht."

Zu bedenken ist stets, dass einer Einwilligung jederzeit mit sofortiger Wirkung widersprochen werden kann. Überlegen sich die Eltern, dass sie doch nicht möchten, dass der Kindergarten Flyer verteilt, in denen ihr Kind abgebildet ist, so können sie widersprechen und der Flyer darf mit sofortiger Wirkung nicht weiter verteilt werden. Das ist natürlich ärgerlich, wenn der Flyer grade frisch aus dem Druck gekommen ist. Widersprechen die Eltern Fotos, die im Netz verteilt wurden, egal ob auf der Homepage des Kindergartens, auf dem YouTube-Kanal, bei Weibo oder Facebook, so ist das Bild beziehungsweise der Beitrag mit dem Bild unverzüglich zu entfernen. Widersprechen sie kurz vor Redaktionsschluss der Veröffentlichung in der lokalen Tageszeitung, so darf die Zeitung das Bild nicht veröffentlichen.

Einwilligungen sollten aktuell sein. Eine Einwilligung für eine Veranstaltung, die erst in drei Jahren stattfindet, ist zu weit in die Zukunft gedacht. Wird sich für die Gestaltung eines Flyers an Fotos von vor drei Jahren erinnert, für die die Betroffenen vor drei Jahren eingewilligt haben, dass die Fotos für Flyer verwendet werden dürfen, so sehen einige Behörden die Einwilligung als zu alt an. Eine Generaleinwilligung für die kommenden drei oder vier Jahre bei der Anmeldung im Kindergarten oder der Schule ist in den meisten Fällen nicht rechtswirksam.

Eine explizite Einwilligung wird nicht benötigt, wenn es ein Gesetz gibt, das ein Lichtbild des Kindes vorschreibt, oder wenn das Foto zum Schutz von Leib und Leben des Kindes dient. Ein Foto bei der Anmeldung, damit Erziehende und Betreuende das Kind identifizieren können, ist sinnvoll. Das lässt sich im Vertrag mit der Betreuungseinrichtung vereinbaren und bedarf dann auch keiner weiteren Einwilligung. Auch bei Gruppenfotos ist eine Einwilligung erforderlich.

Was häufig vergessen wird: Jede Einwilligung bedarf auch der Aushändigung der entsprechenden Informationen nach Art. 13 bzw. 14 DSGVO. Zum einen zur Einwilligung selbst, da hier ja personenbezogene Daten erhoben wurden, als auch für die geplante Fotoaktion. Wobei die Informationen für die Fotoaktion spätestens am Tag, an dem die Fotos gemacht werden, verteilt werden sollte.

Babyfotos bei Gynäkologen

Wer kennt sie nicht? Die vielen Babyfotos bei Gynäkologen und auf Wöchnerinnen-Stationen. Sie geben vielen Frauen Kraft, die Schwangerschaft durchzustehen. Sie symbolisieren, dass auch komplizierte Schwangerschaften zu einem Happy End führen. Die Fotos hauchen den Praxen und den Stationen ein Gefühl von Leben, Glück und Zufriedenheit ein. Wie aber ist das aus Sicht des Datenschutzes?

Alleine, dass diese Frage immer wieder gestellt wird, zeigt, wie groß die Verunsicherung in der Bevölkerung ist. Die Fotos werden von den Eltern an die Praxen beziehungsweise die Stationen geschickt. Die Eltern willigen hier ein beziehungsweise bitten sogar darum, dass die Fotos an den entsprechenden Stellen aufgehängt werden.

Das einzige, was die Praxen und die Häuser beachten müssen, ist, dass sie den Eltern die Informationen entsprechend Artikel 13 DSGVO aushändigen und das Aushängen der Babyfotos in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen wird.

Öffentliche Veranstaltungen

Wenn Kinder bei einem Straßenumzug oder bei einer anderen öffentlichen Veranstaltung, die im Freien auf nicht eingefriedetem Gebiet stattfindet, fotografiert werden und das Foto veröffentlicht wird, ist das etwas schwierig mit der Einwilligung. Die Veranstaltungen sind öffentlich und solange es die Intention des Fotografen ist, die Veranstaltung bildlich festzuhalten und nicht das Kind ist das gesetzlich erlaubt. Wenn die Veranstaltung im eingefriedeten Bereich stattfindet, wie in einem Stadion, braucht sie dafür, dass das Kind ohne Einwilligung fotografiert werden darf, ein großes Maß an öffentlichem Interesse. Beim Tag der Offenen Tür des Kindergartens oder bei der Schulaufführung ist die Einwilligung notwendig.

Kinder veröffentlichen Fotos anderer Kinder

Natürlich passiert es immer wieder, dass Kinder gefragt oder auch ungefragt Fotos von anderen Kindern machen und in den Sozialen Netzwerken verteilen. Hierbei nutzen die Kids heutzutage nicht nur Anbieter aus den USA, wie Facebook, Instagram, WhatsApp und so weiter, sondern gerne auch aus China, wie Weibo und WeChat.

Wenn die Fotos auf dem Gelände einer Betreuungseinrichtung oder während der Betreuung in einer Schule entstanden sind, dann ist die Betreuungseinrichtung beziehungsweise die Schule verantwortlich. Lehrende und Betreuende sollten hier ein Auge darauf haben, dass die Schüler das Fotografier-Verbot einhalten. Es sollte Aufgabe der Erziehenden, sowohl der Eltern als auch der Lehrenden, sein die Kinder stetig zu sensibilisieren.

Fazit

Sensibilisieren von Eltern, Lehrenden und vor allem von Kindern und Jugendlichen ist das A und O. Der langfristig angerichtete Schaden eines unbedacht geposteten Foto eines Kindes kann enorm sein. Schulen, Kindergärten und Betreuungseinrichtungen sind gut beraten, wenn sie das Fotografieren in ihren Einrichtungen verbieten. Wenn Fotos angefertigt werden, ist das zusammen mit dem Prozess der Verarbeitung im Verzeichnis der Verarbeitungstätigkeiten aufzunehmen und die Kinder beziehungsweise die Erziehungsberechtigten müssen die Informationen entsprechend Art. 13 beziehungsweise 14 DSGVO nachweislich erhalten.

Klaus-Jürgen Roth

Digitale Sorge, Mediennutzung und Datenschutz



Bild: ClipDealer

Wie gehen Kinder mit digitalen Medien um? Diese Frage stellt sich nicht nur für Datenschützer, sondern zunehmend auch für Jugendämter und Familiengerichte, die in immer mehr Fällen feststellen müssen, dass bestimmte Formen der Mediennutzung den Kindern schaden, nicht nur durch die unzulässige Verarbeitung personenbezogener Daten. Unsere Rechtsordnung bietet bisher keine spezifischen Antworten, wie diese Schäden verhindert werden können. Deshalb muss auf die allgemeinen Regelungen, insbesondere in § 1626 BGB zurückgegriffen werden, der den **Eltern die Aufgabe und die Pflicht** auferlegt und zugleich das Recht gibt, *für das minderjährige Kind zu sorgen*. Dabei haben sie *die wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbstständigem verantwortungsbewusstem Handeln* zu berücksichtigen.

In den letzten Jahren zog nun das **Amtsgericht Bad-Hersfeld** öffentliche Aufmerksamkeit auf sich, als es in Entscheidungen die elterliche Verantwortung konkretisierte und hervorhob.[1] Allen von diesem Gericht entschiedenen Fällen lagen familienrechtliche Streitigkeiten zwischen getrennt lebenden Eltern zugrunde. Das Gericht lehnte sich bei seinen Beschlüssen oft weit aus dem Fenster, indem es exzessiv hoheitliche Befugnisse für sich in Anspruch nahm und manch aufgezeigte Gefahr für die Kinder übertrieb. Auch entsprachen die Datenschutzargumente des Gerichts nicht immer dem aktuellen Diskussionsstand. Dessen ungeachtet verdienen die Entscheidungen dieses Gerichts eine öffentliche Diskussion.

- Gefahren

Zentrale Frage war in allen Fällen, inwieweit das in § 1666 Abs. 1 BGB geregelte **Kindeswohl** gefährdet ist: *Wird das körperliche, geistige oder seelische Wohl des Kindes oder sein Vermögen gefährdet und sind die Eltern nicht gewillt oder nicht in der Lage, die Gefahr abzuwenden, so hat das Familiengericht die Maßnahmen zu treffen, die zur Abwendung der Gefahr erforderlich sind.*

Dass das Kindeswohl durch die **Nutzung digitaler Medien** gefährdet sein kann, ist heute unbestritten. Die Gefährdung kann darin bestehen, dass hierüber Mobbing stattfindet. Eine spezifische Gefahr liegt in sexuell begründeten Kontaktaufnahmen durch Erwachsene, wobei für das Kind (zunächst) nicht erkennbar sein muss, dass der Kontaktpartner ein Erwachsener ist. Beim Sexting werden Kinder veranlasst, Nacktbilder von sich zu erstellen und diese weiterzuleiten.[2] Schwerwiegende seelische Folgen für die Kinder können pornografische Darstellungen[3] sowie Gewaltpräsentationen und -spiele haben.[4] Nicht nur das private Leben der Kinder, sondern auch deren Schulalltag wird von digitalen Medien beeinflusst.[5] Schließlich ist Online-Sucht ein zunehmendes Problem bei Heranwachsenden[6]; die Abhängigkeit von digitalen Spielen führt zu Realitätsverlusten, dem Verlust sozialer Kontakte sowie zu gesundheitlichen Schäden.

Gefährdungen des Kindeswohls entstehen auch durch **Datenschutzverletzungen.**[7] Applikationsanbieter erstellen über Kinder umfassende Nutzungsprofile, welche die Grundlage für Manipulationen, gezielte Werbung und finanzielle Ausbeutung sind. Das Auslesen von Kontakten und Adresslisten sowie das Ausspionieren von privaten Inhalten, z. B. von Kommunikation, Bildern, dem digitalen Tagebuch[8], kann zu massiven Eingriffen in die soziale Sphäre, in die Intimsphäre oder gar in den Kernbereich persönlicher Lebensgestaltung führen. Informationen aus der Kinderzeit, etwa über seelische oder körperliche Störungen oder über kriminelles Verhalten, können selbst im späteren Erwachsenenalter zu gravierenden Nachteilen führen.[9] Es geht dabei aber nicht nur um Risiken für die Zukunft; möglich sind auch Auswirkungen auf die aktuelle Entwicklung des Kindes und damit auf das Kindeswohl.

- Elterliche Maßnahmen

Mit diesen digitalen Gefährdungen gehen zumeist Eingriffe in das allgemeine Persönlichkeitsrecht und in das Recht auf informationelle Selbstbestimmung der Kinder einher. Oft sind

zudem Kommunikationspartner der Kinder betroffen. Ohne entsprechende **Interventionen der Eltern** sind Kindeswohlgefährdungen oft nicht abzuwenden. Diese Interventionen zielen darauf ab, den Kindern den Zugang zu und die Nutzung von digitalen Inhalten und Kommunikationsmöglichkeiten zu begrenzen und zu gestalten, um übermäßige Gefahren zu vermeiden.

Zur Wahrung ihrer Sorge- und Aufsichtspflichten müssen die Eltern grds. wissen, was ihre Kinder tun und mit welchen Personen sie sich abgeben. Dies gilt nicht nur für die reale analoge Welt, etwa für Kontakte mit Freunden, beim Sport, beim Musizieren oder bei sonstigen Aktivitäten. Dies gilt auch für digitale Kontakte und das Surfen und Spielen im Netz. Bei der dadurch notwendig werdenden **Kontrolle der Kinder** sind diese, soweit dies geht, einzubeziehen (§ 1626 Abs. 2 S. 2 BGB).[10] Die Kontrolle ist ein Eingriff in ihr allgemeines Persönlichkeitsrecht und darf deshalb nicht übermäßig und übergriffig sein. Bei der Kommunikationsüberwachung ist die Integrität des Kindes als eigenständiges Wesen und insbesondere dessen Intimsphäre zu beachten.

Mögliche Formen elterlicher Intervention sind das **Blockieren von Inhalten** und Kontakten, das Deinstallieren von Applikationen[11] oder die Beschränkung des kindlichen Zugriffs auf geprüfte Inhalte[12]. Denkbar ist letztlich auch eine quantitative Begrenzung von Geräten[13] und Nutzungszeiten[14] bis hin zum vollständigen physischen Entzug des Smartphones, Tablets oder sonstigen elektronischen Geräts.

Eine Form der Einflussnahme kann darin bestehen, dass die Eltern am digitalen Kommunikationsverhalten des Kindes beteiligt werden, etwa durch Mitlesenkönnen oder durch Alarmierung in programmtechnisch definierten Verdachts- oder Gefahrenfällen. Dies setzt, da damit in die Grundrechtssphäre des Kindes eingegriffen wird, grundsätzlich dessen Zustimmung voraus. Durch die Einbindung der Eltern wird die Grundlage für einen **Austausch zwischen den Eltern und den Kindern** geschaffen, über den die Risiken eingegrenzt und gegenseitiges Vertrauen aufgebaut werden können.[15]

Genügt ein informeller Austausch nicht, so können Eltern und Kinder gehalten sein, eine **formelle Vereinbarung** über den Umgang mit digitalen Medien zu treffen. Darin können auch bestimmte Sanktionen bei Verstoß gegen die Vorgaben vorgesehen werden.[16] Diese Sanktionen können bis zum Entzug der Nutzungsmöglichkeit des digitalen Geräts gehen. Jede Vereinbarung zwischen Kind und Eltern setzt voraus, dass ihr Inhalt vom Kind nicht nur verstanden, sondern auch akzeptiert wird. Dafür ist es nicht förderlich, wenn die Eltern den Kindern Medienabstinenz abverlangen, selbst aber extensiv diese Medien nutzen. Eltern haben eine Vorbildfunktion, ohne die sonstige pädagogische Maßnahmen zumeist wenig Wirkung zeigen.[17]

- Verhältnismäßigkeit

Die Maßnahmen müssen verhältnismäßig, d.h. auf die Einsichtsfähigkeit und das Alter des Kindes ausgerichtet sein.[18] Sie dürfen dem Kind keine unzumutbaren Einschränkungen abverlangen. So kann z. B. die Deinstallation von Messenger-Diensten, die unter den Freunden des Kindes genutzt werden, eine **kommunikative Isolation** bewirken, die ihrerseits wieder zu einer Kindeswohlgefährdung führen kann.[19] Auf das generelle Kommunikationsverhalten des sozialen Umfelds der Kinder haben die Eltern nur begrenzt Einfluss, doch sollten sie diesen zu nutzen versuchen, etwa über die Schule oder die Elternschaft, um dafür zu sorgen, dass im Umfeld des Kindes generell kindgerechte und datenschutzkonforme Kommunikationsdienste genutzt werden.

Geht ein digitales Angebot mit **Datenschutzverstößen** einher, so wie dies bei dem unter Heranwachsenden weit verbreiteten WhatsApp der Fall ist, so spricht dies für eine Beeinträchtigung des Kindeswohls, ist aber noch kein unwiderlegbares Indiz für eine konkrete Kindeswohlgefährdung i. S. v. § 1666 BGB. Verstöße gegen die Datenschutzrechte Dritter z. B. durch die Nutzung von Kommunikationsdiensten, die unzulässig Adressbücher sowie weitere Daten auslesen, können durch entsprechende Zustimmungen der Kommunikationspartner geheilt werden.[20] Es kann noch keine Gefahr für das Vermögen des Kindes angenommen werden, wenn eine von diesem genutzte Messenger-Applikation unter Verstoß gegen den Datenschutz Daten von Kommunikationspartnern an Dritte weiterübermittelt und damit die Möglichkeit besteht, dass wegen dieses deliktisch-rechtswidrigen Verhaltens Abmahnungen erfolgen und weitergehende Forderungen gestellt werden.[21] Eine Gefahr liegt insofern erst vor, wenn gemäß den Umständen derartige Abmahnungen und Forderungen tatsächlich drohen. Private sind nicht zu einem rechtskonformen Verhalten verpflichtet, schon gar nicht Kinder. Wohl sind sie verpflichtet, die Rechtsfolgen für Rechtsverstöße zu tragen.

Ein grundlegendes Problem bei der digitalen Sorge besteht darin, dass oft die hierfür nötige **elterliche Medienkompetenz** fehlt. Es ist Fakt, dass viele Eltern mit der Technik nicht vertraut sind, die ihre Kinder und zumeist auch sie selbst nutzen. Das Verständnis dafür ist oft begrenzt, erst recht die Kompetenz, die Technik souverän anzuwenden. Insofern sind die Eltern im Interesse der Wahrung des Kindeswohls gehalten, sich die nötige Kompetenz anzueignen oder – soweit dies nicht möglich ist – externe Hilfe in Anspruch zu nehmen.[22]

- Staatliches Wächteramt

Die zwischen Eltern und Kindern bestehende Sorgebeziehung steht gemäß Art. 6 Abs. 2 S. 2 Grundgesetz unter hoheitlicher Aufsicht; die staatliche Gemeinschaft hat hierüber zu wachen. Das Bundesverfassungsgericht (BVerfG) stellt hohe Anforderungen für staatliche **Eingriffe in die elterliche Sorge**. Danach gehört es nicht zur Ausübung des staatlichen Wächteramts, gegen den Willen der Eltern für eine bestmögliche Förderung der Fähigkeiten des Kindes zu sorgen. Die primäre Entscheidungszuständigkeit bezüglich der Förderung ihrer Kinder ist den Eltern zugewiesen.

Für in das Sorgerecht eingreifende Maßnahmen bedarf es einer nachhaltigen Gefährdung des körperlichen, geistigen oder seelischen Wohls.[23] Daraus zieht das Oberlandesgericht Frankfurt/Main den Schluss, dass es für einen staatlichen Eingriff nötig ist, dass der „Eintritt eines Schadens zum Nachteil

des Kindes mit ziemlicher Sicherheit zu erwarten" ist. Auf Grund der Mediennutzung müsse eine **konkrete Gefährdung des betroffenen Kindes** festgestellt werden: „Die Nutzung digitaler Medien muss zum Schutz von Minderjährigen gegebenenfalls pädagogisch begleitet werden; hier ergeben sich individuelle Spielräume, die ... innerhalb der jeweiligen Familien eigenverantwortlich festgelegt werden können." Ein hoheitlicher Eingriff in die Erziehungsmethoden bzgl. der kindlichen Nutzung digitaler Technik ist danach erst zulässig, wenn die Eltern ihrer Verantwortung nicht gerecht werden und festgestellt wird, dass diese auch künftig nicht bereit oder in der Lage sind, eingetretene Gefährdungen abzuwenden.[24]

Hat das **Jugendamt** gewichtige Informationen, die auf eine Gefährdung des Kindeswohls durch digitale Medien hinweisen, so hat es nach Vornahme einer Einschätzung des Gefährdungsrisikos unter Einbeziehung der Erziehungsberechtigten und des Kindes bzw. Jugendlichen gemäß § 8a Abs. 1 SGB VIII eine Lösung zu suchen. Als Maßnahmen kommen familiengerichtliche Anordnungen nach § 1666 Abs. 1 BGB in Betracht, mit denen die Gefahr für das Kindeswohl abgewehrt werden kann. Eine solche Anordnung kann auch auf Initiative des Jugendamtes gemäß § 8a Abs. 2 SGB VIII erfolgen.

- Forschungsbedarf

Die Pädagogik zur Mediennutzung von Kindern befindet sich in der Entwicklung. Die Erforschung der seelischen, gesundheitlichen und sozialen Konsequenzen der Nutzung digitaler Techniken durch Heranwachsende befindet sich noch in den Kinderschuhen. Staatliche Maßnahmen, mit denen Eingriffe in die geschützte Beziehung zwischen Eltern und Kindern erfolgen, auch wenn es darum geht, den Datenschutz zu sichern, bedürfen nicht nur einer rechtlichen Grundlage, sondern auch einer faktischen Rechtfertigung. Insofern besteht noch sehr großer Bedarf an belastbaren **Erkenntnissen**. Auf Grundlage des erlangten Erfahrungswissens ist es dann auch sinnvoll, weitere normative Vorgaben festzulegen. Nötig ist aber auch, dass die bestehenden rechtlichen Regelungen durch die staatliche Aufsicht gegenüber den Anbietern durchgesetzt werden. Dies gilt für den Jugendschutz wie für den Datenschutz. Der Ansatz, illegale Angebote wie z. B. WhatsApp über das elterliche Sorgerecht zu bekämpfen, so wie dies offenbar das AG Bad Hersfeld versucht, kann keinen nachhaltigen Erfolg haben.

1 AG Bad Hersfeld 22.07.2016 – F 361/16 EASO (1), K&R 2016, 621; AG Bad Hersfeld 20.03.2017 – F 111/17 EASO (2); AG Bad Hersfeld 15.05.2017 – F 120/17 EASO (3); AG Bad Hersfeld 10.01.2018 zitiert bei OLG Frankfurt 15.06.2018 – 2 UF 41/18.

2 Großekathöfer, Für immer nackt, Der Spiegel 7/2018, 54-58.

3 Bauschmüller/Braun, „Schon Drittklässler erzählen mir von Pornos", Interview mit von Weiler, SZ 29.01.2019, 8.

4 AG Bad Hersfeld 27.10.2017 – 63 F 290/17 SO.

5 Linnartz, Das ewige Klassenzimmer, SZ 13.05.2019, 12.

6 Kreye, Macht süchtig, SZ 09./10.2019; AG Bad Hersfeld (3) S. 26.

7 AG Bad Hersfeld (1), S. 16 f.

8 AG Bad Hersfeld (1), S. 20; AG Bad Hersfeld (3), S. 22.

9 AG Bad Hersfeld (3), S. 28.

10 AG Bad Hersfeld (3), S. 23.

11 Zu WhatsApp ausführlich AG Bad Hersfeld (1), S. 16 ff.; AG Bad Hersfeld (2).

12 AG Bad Hersfeld (1), S. 20 u. a. mit weitergehenden technischen Hinweisen.

13 AG Bad Hersfeld (1), S. 21.

14 AG Bad Hersfeld (3), S. 25 f.

15 AG Bad Hersfeld (1), S. 19; AG Bad Hersfeld (3), S. 22.

16 AG Bad Hersfeld (3) S. 2, 27; vgl. www.mediennutzungsvertrag.de; www.internet-abc.de/Eltern/familie-medien/; www.schau-hin.info.

17 AG Bad Hersfeld (3), S. 26 f.

18 AG Bad Hersfeld (1), S. 18.

19 AG Bad Hersfeld (1), S. 22, einschränkend aber S. 23.

20 AG Bad Hersfeld (3), S. 2, 21.

21 So AG Bad Hersfeld (2), S. 5, 19 ff. unter Verweis auf die §§ 823, 828, 1004 analog BGB; ebenso AG Bad Hersfeld (3), S. 6, 10 ff.

22 AG Bad Hersfeld (1), S. 18 f.; AG Bad Hersfeld (3), S. 3, 25.

23 BVerfG 20.01.2016 – 1 BvR 2742/15, Rn. 12, FamRZ 2016, 439.

24 OLG Frankfurt/Main 15.06.2018 – 2 UF 41/18, Rn. 25; FuR 2018, 612 = MDR 2018, 1190 = MMR 2019, 253.

Heinz Alenfelder

Online-Spiele: Was geschieht mit den Daten – Ein Überblick und einige Empfehlungen

Spiele und das Online-Spielen sind in unserer Gesellschaft auf dem Vormarsch. Dank der modernen digitalen Technologie kann heute in fast allen Lebenslagen gespielt werden. Wissenschaftlich beschäftigen sich die Beiträge im Online-Sammelband „Digitale Spiele im Diskurs", der seit 2015 im Rahmen der Reihe „Medien im Diskurs"[1] der FernUniversität in Hagen erscheint, mit dieser Entwicklung. Was dort bisher fehlt, ist der Blick auf den Datenschutz. Auch die Spielenden sind in aller Regel ratlos, wenn sie denn überhaupt ein Bewusstsein für dieses Thema entwi-


Bild: Shutterstock

ckeln, und bestätigen endlos lange Datenschutzerklärungen, meist ohne sie überhaupt gelesen zu haben.

Dieser Artikel soll nun zunächst – frei nach Friedrich von Schiller („Wer zählt die Pannen, nennt die Namen, die hier nun schon zusammen kamen?") – mit einem chronologisch sortierten Überblick einiger „Datenskandale" aus der modernen Online-Spielewelt die Problematik der beim Spielen anfallenden Datenmengen anreißen. Darauf folgen Beispiele für das, was Industrie und Forschung aus Spiele-Daten herauslesen können und wollen. Abschließend werden Ergebnisse der Suche nach möglichst konkreten Empfehlungen an Spielerinnen und Spieler für den Umgang mit dem Datenschutz vorgestellt.

In der DANA wurden elektronische Spiele erstmalig 2012 anlässlich der Verleihung des Big Brother Awards an Blizzard Entertainment erwähnt[2]. Das zweite Mal nahmen Frank Spaeing und Roland Appel 2016 das „Phänomen Pokémon GO"[3] unter die Lupe. Sie beschrieben einerseits die konkreten Details dieses Spiels, um das sich in aller Schnelle ein Hype entwickelt hatte, und setzten sich andererseits damit auseinander, wie bedenkenlos Spielende ihre Daten an die Spieleherstellerfirmen abgeben. Darüber hinaus wurde – nicht nur seitens der DVD – die Unmöglichkeit des anonymen Spiels bei Pokémon GO bemängelt[4].

Kleine und große Datenpannen aus der Welt der Spiele

Sicherlich einer der zahlenmäßig größten Skandale in der Spiele-Welt betraf **2011** das Sony-Netzwerk. Seinerzeit wurden 77 Millionen unverschlüsselter Account-Daten entwendet[5]. Ein Blog auf der österreichischen Webseite Techbold.at führt im Zusammenhang mit der DSGVO die PlayStation auf dem zweiten Platz der Datenpannen auf. Damals waren lediglich die Kreditkartendaten verschlüsselt und das Netzwerk musste abgeschaltet werden, was Sony nach eigenen Aussagen eine dreistellige Millionensumme in Euro kostete.

Bereits 2005 erhielt Blizzard Entertainment den österreichischen Big Brother Award in der Kategorie „Kommunikation und Marketing" für das Ausspionieren von Arbeitsspeichern und Rechnerdaten. **2012** folgte für dieselbe Firma dann der deutsche Big Brother Award in der Kategorie „Verbraucherschutz"[6], weil für die Spiele-Accounts im Freundschaftssystem Real ID statt Phantasie-Namen nur noch öffentliche reale Klarnamen zur Anmeldung verwendet werden sollten. Nach den damaligen Bedingungen verzichteten Spielende sogar auf „alle Persönlichkeitsrechte, die Sie ggf. in Bezug auf Nutzerinhalte haben".

Der Spielzeug- und Lernsoftware-Hersteller VTech wurde im November **2015** gehackt.[7] Dabei wurden auch Daten von über sechs Millionen Kindern entwendet, mehr als 500.000 davon in Deutschland. Adressen, Namen und Geburtstage konnten in Verbindung mit Eltern-Konten gebracht werden. Der Spielzeughersteller verkündete damals, Bankverbindungsdaten seien nicht erbeutet worden. Anfang 2018 verhängte die US Federal Trade Commission (FTC) in dieser Sache eine Strafe von $ 650.000 gegen VTech, was etwa 22 Cent pro betroffenem Kind ausmacht.[8]

Nicht nur Spiele-, sondern auch TV-Nutzungsdaten sind für das Schalten von Werbespots interessant. Diese Daten werden, so ein Artikel der New York Times vom Jahresende **2017**[9], von einer Software des Silicon Valley-Start-Ups Alphonso in über 1000 Smartphone-Applikationen gesammelt. Dazu gehören auch viele Spiele-Apps, die sich zum Teil speziell an Kinder richten. Selbst wenn die entsprechende App gerade nicht genutzt wird, analysiert das Mikrofon des Smartphones Umgebungsgeräusche und kann speziell in Werbespots eingelagerte Tonfolgen registrieren. Die Autorin des Artikels, Sapna Maheshwari, berichtet darüber hinaus, dass die US-amerikanische Handelskommission 2017 gegenüber Entwicklern der Software Silver Push eine Rüge aussprach, weil die Software für Menschen nicht hörbare Töne in Fernsehsendungen analysierbar machte[10]. Das entsprechende Patent liegt seit 2015 in den Händen von Facebook. Dort, so die österreichische Webseite derstandard.de, betont man allerdings, es solle „niemals zum Einsatz kommen".[11]

Anfang **2018** wurden Mängel bei der Authentifizierung des Spiels *Fortnite* (Epic Games) bekannt, die angreifenden Hackern die Möglichkeit boten, Artefakte und Geld aus dem Spiel zu entwenden.[12] Insbesondere V-Bucks, die im Spiel verwendete Währungseinheit, hätte gestohlen und in der realen Welt zu Geld gemacht werden können. 2019 geriet Epic Games wiederum in die Kritik. Im Dezember des Vorjahres hatte der Spielehersteller eine eigene Gaming-Plattform veröffentlicht, um vor allem der Plattform Steam Konkurrenz zu machen. Im März 2019 wurde nun behauptet, der Spiel-Launcher sammle auf der Plattform Steam Daten von Spielenden und leite sie an Epic Games weiter. Das Unternehmen könne die Daten dann für eigene Zwecke nutzen[13].

Die Webseite gamestar.de berichtete im Februar **2019**[14], dass zu *Apex Legends*, einem Spiel von Respawn mit 25 Millionen Mitspielenden, bereits in der ersten Woche nach Erscheinen eine Fake-App erschien. Diese App versprach beste Spielerlebnisse auf Mobilgeräten, was allerdings zu diesem Zeitpunkt gar nicht möglich war. Statt dessen war die App mit Adware ausgestattet, die den Entwicklern Geld für (unfreiwillig) heruntergeladene Werbung in die Kasse spült. Dieselbe Methode war schon bei *Fortnite* und *Pokémon Go* angewendet worden.

Die im Juni **2019** bei vox.com veröffentlichte „history of mobile game data collection"[15] schließlich bezeichnet das seit 2009 erfolgreiche Spiel Angry Birds der finnischen Firma Rovio als Trojanisches Pferd. Die Autorin, Kaitlyn Tiffany, bezeichnet die Veröffentlichung des Spiels als Beginn einer Dekade, in der freie Apps auf das Smartphone heruntergeladen werden, „without having any real idea what they were getting from us". Edward Snowden habe 2014 gezeigt, dass die amerikanische National Security Agency (NSA) nicht nur mit *World of Warcraft*, sondern auch mit *Angry Birds* private Daten ausspionierte[16]. Den entwickelnden Firmen sei in der Regel nicht einmal klar, welche Daten von wem gesammelt würden, da sie bei der Entwicklung auf Third-Party-Werbe-Software zurückgreifen (häufig von bekannten Firmen wie Facebook, Google oder Twitter, oft aber auch von einem Dutzend weiterer Unternehmen). Tiffany warnt vor dem Einwand, Spiele-Daten seien harmlos, denn Studien würden zeigen: „you play games differently when you're depressed, or dieting". Sehr kritisch sind vor allem Persönlichkeitsprofile zu bewerten, die nach einem US-Patent von 2007 aus den Spieldaten gewonnen werden können.

Jüngst machte Electronic Arts im Oktober **2019** durch eine Panne beim Registrieren für die „FIFA 20 Global Series" auf sich aufmerksam. Laut der Webseite pcgameshardware.de[17] waren im Anmeldeformular von etwa 1600 Personen fremde Accountdaten sichtbar. Neben Geburtsdaten sollen sowohl E-Mail-Adressen und ID-Kennungen als auch Länderangaben bereits eingetragen gewesen sein. Das Formular wurde nach 30 Minuten deaktiviert, doch obwohl das Problem bei Twitter schnell kommuniziert worden war, dauerte es mehrere Stunden, bis sich EA dazu äußerte.

Mit diesen sich scheinbar immer häufiger ereignenden Datenpannen ist nur die Spitze eines Eisbergs gezeichnet, der in seiner vollen Bedeutung kaum zu unterschätzen ist. Die Aufzählung von Skandalen allerdings wird der Datenschutz-Problematik nicht gerecht, wie bereits das im vorletzten Abschnitt erwähnte US-Patent zu Persönlichkeitsprofilen zeigt.

Wer sammelt eigentlich wessen Daten und wozu? – Ein Blick in die Forschung

Nach dem von einem Google-Mitarbeiter registrierten Patent[18] können „Spieleigenschaften, die im Chat verbrachte Zeit, das Verhalten beim Tauschhandel, die Erforschung von Gebieten, die Entscheidung bei Konfliktsituationen" und weitere Daten für Werbung genutzt werden. Also gilt es, über die aktuellen Pannen hinaus anzuschauen, was prinzipiell mit Daten von Spielenden geschehen kann, wie sie genutzt werden können und durchaus auch genutzt werden.

Aussagen über die Persönlichkeit von Spielenden erforschte schon **2015** eine Studie zum Spiel *League of Legends*[19]. Kokkinakis, Lin, Pavlas und Wade arbeiten darin Zusammenhänge zwischen „anti-sozialen" Namen der Spielcharaktere, dem sozialen Verhalten der Mitspielenden und deren Alter heraus. Das Forschungsteam vermutet, dass positives Verhalten in der Spielumgebung („rapid learning, team-building or leadership") sowohl mit positiven Spielernamen als auch mit positiven Persönlichkeitseigenschaften in der Realität korreliert. Es kündigte an, sich weiterhin damit zu beschäftigen, inwieweit eine Verstärkung altruistischer Strategien in einer Spielumgebung ein antisoziales Verhalten im Alltag beeinflussen kann.

Im kanadischen Toronto Star erschien Ende **2015** ein Artikel von Alex Boutilier[20], in dem dieser nicht nur beschreibt, welche personenbezogenen Daten von Spielefirmen gesammelt werden, sondern auch ein eindrucksvolles Beispiel für die Verwendung der Daten durch einen Spieleanbieter über das Marketing hinaus vorstellt. King, der Hersteller der äußerst erfolgreichen Serie *Candy Crush*, stellte demnach durch Datenauswertung fest, dass viele App-Nutzer beim Level 65 mit dem Spielen aufhörten. Als Reaktion wurde dieses Level einfacher gestaltet und schon spielten die Spielerinnen und Spieler sehr viel länger mit der kostenfreien App.

Allgemein scheinen Angehörige der jungen Generationen wohl durchaus bereit, Daten gegen kleine Belohnungen herauszugeben. So wurden **2017** am Massachusetts Institute of Technology (MIT) mehr als 3000 Studierende in einer Studie aufgefordert, E-Mail-Adressen aus dem nahen Freundeskreis weiterzugeben[21]. Aus der Gruppe, der als Belohnung eine kostenlose Pizza winkte, gaben 98 % der Studierenden E-Mail-Adressen weiter, in der Kontrollgruppe ohne Belohnung waren es 94 %. Hier waren allerdings in 6 % der Fälle die E-Mail-Adressen gefälscht.

2017/2018 wurde das Gebiet „Privacy in Gaming" in einer Studie am Center of Law and Information Policy (CLIP) an der Fordham Law School umfassend analysiert[22]. Die Studie untersuchte nicht nur die häufigsten Spiele in den App-Stores von Apple und Google, sondern auch die verschiedenen Spielgeräte und deren Zubehör (Kamera, Sensoren, Mikrofon, etc.). Alle untersuchten Plattformen und Spiele verwenden die gesammelten Daten für Werbezwecke. Die Autoren der Studie beklagen die Intransparenz des Datenaustauschs: „Transparency as to gaming companies' data sharing practices could be much improved".

2018 berichtet die Deutsche Telekom über die Unterstützung der wissenschaftlichen Auswertung von Spieler-Daten[23]. Im Demenz-Forschungsprojekt *Sea Hero Quest*, einer Spiele-App, die weltweit vier Millionen Installationen umfasst, wurden Daten von Spielerinnen und Spielern, die Alter, Geschlecht und Nationalität angegeben hatten, auf den Zusammenhang zwischen materiellem Wohlstand, Grad der Gleichstellung der Geschlechter und räumlichem Orientierungsvermögen untersucht. Im Ergebnis wurde festgestellt, dass bei höherem materiellem Wohlstand das Orientierungsvermögen besser ist (Skandinavien, Nordamerika, Australien und Neuseeland schnitten am besten ab; Indien, Ägypten und Irak deutlich schlechter). Männer erzielten durchschnittlich bessere Ergebnisse als Frauen; der Unterschied sinkt mit besserer Gleichstellung im Heimatland. Generell wollen die Forscher mit der Datenanalyse auch Verfahren entwickeln, die der Medizin die frühzeitige Diagnose räumlicher Desorientierung ermöglicht.

Kevin Townsend berichtet im Blogbeitrag „Gamers and Gaming Security" des tschechischen Sicherheitssoftware-Herstellers Avast[24], dass laut einer US-amerikanischen Umfrage von Anfang **2019** 55 % der Spielenden dasselbe Passwort auf verschiedenen Accounts nutzen und durchschnittlich 5 Cyberattacken erlebt haben. Townsend macht klar, dass innerhalb der Spieleumgebungen virtuelle Gegenstände von Hackern gestohlen und in der realen Welt für reales Geld verkauft werden können. Er stellt bezüglich des erstaunlichen Vertrauens, das Spielende den Spielefirmen entgegenbringen, fest: „While video games are entertainment, players often trust as much of their personal information to game companies as they would to their workplace, to online shopping or even to financial institutions." Neben den virtuellen Gegenständen interessieren sich die Diebe vor allem für Daten wie Ortsangaben, Mediennutzungsgewohnheiten, Telefondaten und natürlich auch für finanzielle Informationen, die zum Begleichen von Käufen innerhalb der Spiele hinterlegt wurden. Townsend zählt die Angriffspunkte auf: schwache Authentifizierung, vielfältige Veröffentlichung von Spieler-Namen, Phishing und Malware. Neben den Spielenden sieht er auch die Spielefirmen in der Pflicht, für mehr Sicherheit zu sorgen, beispielsweise durch das Angebot einer Zwei-Faktor-Authentifizierung und einer schnellen Unterstützung im Schadensfall. Interessant, doch keinesfalls unstrittig ist seine Einlassung zur verhaltensorientierten Biometrie (behavioral biometrics), für die er im Spieleumfeld eine „unique position to explore the technology" sieht. In Ansätzen wird diese Technik heute in Cheat-Erkennungs-Systemen eingesetzt, die Falsch-Spielerei entlarven sollen. Unbeachtet bleibt im Blogbeitrag die dabei neu entstehende Sammlung sensibler Daten.

Wie einfach es für Hacker sein kann, die modernen sprachanalysierenden Boxen von Amazon (Alexa) oder Google (Home) zum Datensammeln zu animieren, zeigen aktuelle Berichte des Berliner Forschungsinstituts Security Research Labs[25] vom Oktober **2019**. Danach gelang es dem Forschungsteam, abhörende Apps (Skills für Alexa bzw. Actions für Home) in die jeweiligen App-Stores zu bringen. In weitergehenden Versuchen konnten diese Apps die Nutzenden sogar dazu bringen, das Passwort laut auszusprechen.

Jüngst veröffentliche Forschungsergebnisse aus **2019** belegen auch, dass das Bewusstsein über die Problematik der Weitergabe von personenbezogenen Daten bei den meisten Betroffenen erst geweckt werden muss. Beim Einsatz eines Privacy-Themas in einem Spiel für Smartwatches, so stellte ein Team um Meredydd Williams von der Universität Oxford in einer Studie fest, wurden signifikant datenschutz-freundlichere Einstellungen an der Uhr vorgenommen, als ohne dieses Kapitel.[26] Damit zeigt sich also, dass Veränderungen möglich sind, wenn sie in der passenden Form an die Spielenden herangetragen werden und diese entsprechend ermutigen, Datenschutz ernst zu nehmen. In eine ähnliche Richtung geht auch die neuseeländische Webseite www.privacygames.com, die spielerisch in das Thema Datenschutz einführen und Bewusstsein schaffen will.

Auf der Suche nach Empfehlungen für Spielende

Mit dem Bewusstsein alleine ist es noch nicht getan. Zwar fordert der im vorletzten Absatz erwähnte Blogger Townsend Spielefirmen explizit zu Sicherheitsmaßnahmen und zur Datensparsamkeit auf: „Game companies, as with any organization gathering or storing data on its customers, should follow best practices for security and never gather more data than is necessary", doch ist zu prüfen, was die Spielerinnen und Spieler über das Akzeptieren der Datenschutzbedingungen hinaus selbst tun können. Empfehlungen hierzu sind rar gesät. Einige Recherche-Ergebnisse sollen dennoch abschließend vorgestellt werden.

2010 veröffentlichte das Unabhängige Landeszentrum für Datenschutz Schleswig Holstein (ULD) einen Leitfaden „Datenschutz in Online-Spielen", den es im Auftrag des Bundesministeriums für Bildung und Forschung entwickelt hatte. Aufgrund des Alters der Studie ist zwar zu prüfen, wie aktuell der Leitfaden ist, allerdings sind die grundsätz-

lichen Erwägungen auch heute noch relevant. So wird festgestellt, dass zu den personenbezogenen Daten „neben Bestandsdaten wie Name, Adresse etc. u. a. auch Daten, die Rückschlüsse auf das Verhalten des Spielers erlauben", gehören. Weiter gibt der Leitfaden Anregungen für die Entwicklung von Spielen und wies schon damals auf Datensparsamkeit und das Prinzip „Privacy by Default" hin. Einige Module sind vor allem deshalb für Nicht-Spielerfahrene interessant, weil sie den Fokus auf übliche Spielsituationen lenken und Lösungen anreißen:

- Spieler-zu-Spieler-Erkennbarkeit (Freundeslisten etc.) – Lösung durch Pseudonyme und gesonderte Einwilligung, Forderung nachträglicher Informationsmöglichkeit
- Reputationssystem (Bewertung anderer Mitspielenden) – Lösung durch transparentes Beschwerdeverfahren, Verzicht auf schwarze Listen, automatische Alterungsprozesse für Bewertungen
- Highscorelisten (Präsentation von Spielergebnissen) – Lösung durch Transparenz, Einwilligung, Pseudonyme und Alterungsprozess.

Offizielle Seiten tun sich bisher schwer mit Empfehlungen. So heißt es beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zum Thema Computerspiele in der Rubrik „BSI für Bürger", dass „Schadsoftware über Phishing-Mails, USB-Sticks, Downloads, Werbebanner oder das Spiel selbst auf den Rechner" gelangen kann und dass die „eingegebenen Login-Daten an eine externe Adresse verschickt" werden können[27]. Schwache Passworte werden als eine der wesentlichen Lücken benannt. Die Tipps sind eher schlicht und dürften selbstverständlich sein: Spiele nur aus offiziellen Quellen laden, Verknüpfung mit sozialen Medien vermeiden, Passwortsicherung für In-App-Käufe, regelmäßige Updates der Spiele und Einrichtung eines gesonderten Benutzeraccounts auf dem PC. Fraglich ist in diesem Zusammenhang aber, wie der folgende Tipp zum Accountschutz überhaupt umgesetzt werden kann: „Erstellen Sie einen Account nur, wenn Sie absolut sicher sind, dass Ihre Daten vertraulich behandelt werden und mit einer entsprechenden Verschlüsselungstechnik vom Anbieter gesichert sind." Auch der Verein „Deutschland sicher im Netz e. V."[28] kommt beim Datenschutz kaum über den Hinweis „Lesen Sie die Datenschutzerklärung von Spielen" hinaus. Immerhin empfiehlt er explizit das Überprüfen von Berechtigungen, insbesondere bei Spiele-Apps.

In Österreich hat das Institut für Technikfolgen-Abschätzung 2017 das Projekt „Datenschutz in Online-Spielen – Spielend Daten sammeln"[29] durchgeführt. Der sehr ausführliche, lesenswerte Abschlussbericht stellt das Problemfeld umfassend dar und gibt auch Empfehlungen an Nutzerinnen und Nutzer. Diese reichen von „Kinder beaufsichtigen" über „Schadsoftware vermeiden" bis zum sparsamen Umgang mit den eigenen Daten (Adresse, Telefonnummer, Kreditkarten-Nummern) und dem Löschen des Accounts, wenn das Spiel nicht mehr genutzt wird.

Ein weiterer Blick über die deutschen Grenzen hinaus zeigt auf der Webseite der schweizerischen Goldenfrog GmbH in einem „Gamer's Guide to Online Privacy and Security"[30] eine neue Community #GamersForPrivacy. Zwar handelt es sich bei dem „Wegweiser" um eine Werbung für die Software *vyprvpn*, doch werden auch hier die Risiken klar benannt: Veröffentlichung der IP-Adresse sowohl gegenüber dem Internet-Service-Provider als auch dem Anbieter für die Telekommunikation (als Beispiel wird hier Skype erwähnt). Außerdem wird auf die in DANA 1/2019 erwähnte Website *Have I Been Pwned* (S. 48) hingewiesen und die Empfehlung für Phantasie-Namen, unterschiedliche Passworte und Zwei-Faktor-Authentifizierung ausgesprochen. Der Beitrag liefert auch gleich zu gängigen Spielen die passenden Web-Adressen der Spielhersteller.

Die Kanadische Datenschutzbehörde erklärt in einem aktuellen Dokument „Gaming and personal information: playing with privacy"[31] das Thema Online-Spiele nicht nur, sondern untermauert es auch mit vereinzelten Tipps. Auch hier lautet die erste Empfehlung, für Spiele eigene E-Mail-Adressen anzulegen, weil damit eine Mail-Adressen-Weitergabe durch die Herstellerfirma zumindest nachvollziehbar wird. Natürlich bleibt der Hinweis nicht aus, insbesondere vor Koppelung des Spiele-Accounts mit einer Social-Media-Plattform die Nutzungsbedingungen und Datenschutz-Regelungen aufmerksam zu lesen und die Einstellungen so restriktiv wie möglich zu gestalten. Doch es bleibt dabei: „If you're not comfortable, don't sync them". Die Behörde problematisiert auch die Einverständniserklärung durch die Eltern von Kindern (für Kanada unter 13-Jährige).

Verschiedene Zeitschriften und Blogs für Gamer informieren in kleinen Beiträgen über das Problem der Sicherheit beim Spielen und geben nebenbei auch Tipps. So beispielsweise Gamestar[32]: „Zwei-Faktor-Authentifizierung ist eine einfache Methode, um die eigene Sicherheit weiter nach oben zu schrauben, frische Updates sollten sowieso


Bild: Shutterstock

möglichst zeitnah installiert werden." Recht umfassend informiert schließlich die Webseite www.klicksafe.de über das gesamte Feld der digitalen Spiele[33]. Ein detaillierter Abschnitt beschäftigt sich mit dem Datenschutz. Allerdings bleibt auch hier offen, wie das Grundproblem gelöst werden kann. So folgt etwa auf die richtige Feststellung „Zudem übertragen manche Kopierschutzvorrichtungen persönliche Daten, ohne dass ersichtlich wird, was mit ihnen passiert" die Aufforderung „Lies in den AGBs, bzw. der Datenschutzerklärung nach, was der Anbieter mit Deinen Daten macht!"

Zusammengefasst ergeben sich also folgende Empfehlungen:

- Spiele sollten nur aus offiziellen Quellen geladen und per Update immer zeitnah aktualisiert werden.
- Auf einem PC oder Tablet ist für Spiele ein gesonderter Benutzeraccount einzurichten.
- An erster Stelle der Sicherheitsmaßnahmen steht die Verwendung eines Pseudonyms und eines starken Passworts. Eine Zwei-Faktor-Authentifizierung wird empfohlen.
- Kreditkartendaten sind nur dann anzugeben, wenn auch wirklich In-Game-Käufe vorgenommen werden.
- Sowohl Pseudonym als auch gesonderte E-Mail-Adresse und Passwort sollen für jedes Spiel unterschiedlich sein.
- Bei Spiele-Apps sind die Einstellungen bezüglich Kamera, Mikrofon und GPS-Zugriff zu prüfen und möglichst restriktiv zu beschränken.
- Auf eine Verknüpfung mit sozialen Medien sollte verzichtet werden.
- Wenn das Spiel/die App nicht mehr benutzt wird, sollte der Account aktiv gelöscht werden.

Am Ende aber kommt niemand umhin, die Datenschutzerklärungen der Spieleanbieter zu studieren und sich gegebenenfalls gegen ein Spiel zu entscheiden. Eine weitere Möglichkeit besteht darüber hinaus darin, die Rechte nach der DSGVO einzufordern, so beispielsweise das Recht auf Auskunft über die gespeicherten, personenbezogenen Daten. Ebenso verdient mittelfristig das Schulungs- und Lernangebot an die jungen Generationen, wie es beispielsweise die neuseeländische Seite www.privacygames.com macht oder wie es Johannes Georg Thielen mit einer Unterrichtsreihe in seiner Masterarbeit[34] herausarbeitet, eine besondere Beachtung. Entsprechende Beiträge unserer Leserschaft sind gern gesehen, auch wenn wir uns den Abdruck vorbehalten.

1 Fernuniversität in Hagen, Lehrgebiet Bildungstheorie und Medienpädagogik, Prof. Dr. Claudia de Witt https://www.fernuni-hagen.de/bildungswissenschaft/bildung-medien/medien-im-diskurs/digitale-spiele.shtml

2 DANA 2/2012, 70

3 DANA 3/2016, 134-144

4 Heise-Kurzlink https://heise.de/-3269009

5 https://www.techbold.at/blog/datenpannen

6 https://bigbrotherawards.de/2012/verbraucherschutz-blizzard-entertainment

7 https://www.spiegel.de/netzwelt/games/vtech-hack-noch-groesser-profile-von-509-000-kindern-in-deutschland-erbeutet-a-1065606.html

8 https://www.theregister.co.uk/2018/01/08/vtech_ftc_settlement_hacking/

9 https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html

10 siehe: Heise-Kurzlink https://heise.de/-3704642

11 https://derstandard.at/2000082478721/Facebook-patentiert-heimliches-Mithoeren-mittels-Mikrofon

12 https://blog.avast.com/cybersecurity-risks-all-gamers-should-know

13 https://www.4players.de/4players.php/spielinfonews/PC-CDROM/40293/2181587/Epic_Games_Store-Epic_Games_reagiert_auf_Datenschutz-Kritik_sowie_Spionage-_und_Spyware-Vorwuerfe.html

14 https://www.gamestar.de/artikel/apex-legends-achtung-erste-fake-app-aufgetaucht-die-malware-installiert,3340722.html

15 Kaitlyn Tiffany, https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

16 https://www.br.de/puls/themen/netz/datenspionage-bei-computerspielen-der-glaeserne-gamer-100.html

17 https://www.pcgameshardware.de/FIFA-20-Spiel-62173/News/Registrierungsformular-fuer-Global-Series-zeigte-fremde-Daten-1334014

18 https://bigbrotherawards.de/2012/verbraucherschutz-blizzard-entertainment

19 https://www.sciencedirect.com/science/article/pii/S0747563215301655

20 Alex Boutilier, Video game companies are collecting massive amounts of data about you https://www.thestar.com/news/canada/2015/12/29/how-much-data-are-video-games-collecting-about-you.html

21 Kari Paul, Americans are worried about their Facebook data ... https://www.marketwatch.com/story/college-students-would-give-up-their-friends-privacy-for-free-pizza-2017-06-13

22 https://ssrn.com/abstract=3147068

23 https://www.telekom.com/de/medien/medieninformationen/detail/deutsche-telekom-bewirkt-wichtige-fortschritte-in-der-demenzforschung-539748

24 https://blog.avast.com/cybersecurity-risks-all-gamers-should-know

25 https://srlabs.de/bites/smart-spies/

26 Meredydd Williams, Jason R.C. Nurse, Sadie Creese, Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study http://www.sciencedirect.com/science/article/pii/S0747563219301748

27 https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Gaming_mit_Sicherheit.html

28 https://www.sicher-im-netz.de/gaming-auch-beim-spielen-sicher-bleiben

29 http://epub.oeaw.ac.at/?arp=0x0036ea15

30 https://www.goldenfrog.com/vyprvpn/guides/gamers-guide-online-privacy-security

31 https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/gd_gc_201905/

32 https://www.gamestar.de/artikel/security-tipps-fuer-spieler-accounts-und-system-schuetzen,3327506,fazit.html

33 https://www.klicksafe.de/themen/digitale-spiele/digitale-spiele/rechtliche-aspekte/datenschutz/

34 https://kola.opus.hbz-nrw.de/opus45-kola/frontdoor/deliver/index/docId/1831/file/Masterarbeit.pdf

Anne Riechert

Die Vernetzung von Patientendaten im Gesundheitssystem

I. Einleitung

Eine zentrale Patientendatei, am besten europaweit? Wie sehen die bisherigen und die geplanten Änderungen zum Sozialgesetzbuch V aus und was beinhalten Begriffe wie Telematikinfrastruktur, Patientenakte, Gesundheitsakte und Gesundheitskarte? Kritiker befürchten ein Paradies für die Pharmaindustrie und beklagen eine „Zwangsvernetzung" von Leistungserbringern, wie Ärzten oder Psychotherapeuten.[1] Andere sehen die Möglichkeit, zukünftig die Gesundheitsversorgung aufgrund umfassender Vernetzung und Digitalisierung des Gesundheitswesens bestmöglich sicherzustellen und zu optimieren.

Im Fokus der öffentlichen Diskussion steht derzeit die so genannte Telematikinfrastruktur, eine Vernetzung von Krankenkassen, Ärzten sowie anderen Leistungserbringern, um Patientendaten schnell und unkompliziert verarbeiten zu können. Im Sozialgesetzbuch V ist diesbezüglich geregelt, dass die *Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH* (gematik) die Rahmenbedingungen für den Betrieb dieser Telematikinfrastruktur festlegt und deren Einhaltung überwacht. Gesellschafter sind u.a. das Bundesministerium für Gesundheit, Ärztekammern und Krankenversicherungen.[2] Die Gesellschaft für Telematik nimmt darüber hinaus ebenso auf europäischer Ebene Aufgaben wahr und soll zukünftig darauf hinwirken, dass die für den grenzüberschreitenden Austausch von Gesundheitsdaten erforderlichen Festlegungen mit den Vorgaben für die Telematikinfrastruktur sowie mit den europäischen Vorgaben vereinbar sind.

Basis der Vernetzung stellt die elektronische *Gesundheitskarte* dar, auf der Stammdaten eines Patienten (z.B. Name, Adresse, Geburtsdatum) gespeichert sind und die insgesamt geeignet sein muss, eine elektronische Patientenakte zu unterstützen. Davon abzugrenzen ist die so genannte elektronische *Gesundheitsakte*, die eine freiwillige Leistung der Krankenkassen darstellt.

II. Verarbeitung von Gesundheitsdaten

Im vorliegenden Kontext sind die Regelungen des Sozialgesetzesbuches V (SGB V) maßgebend, die durch Artikel 1 – Terminservice- und Versorgungsgesetz (TSVG)[3] bereits mit Wirkung ab 11.05.2019 geändert worden sind. Der Entwurf des Bundesministeriums für Gesundheit („Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation", Digitale-Versorgung-Gesetz) sieht nun weitere Änderungen vor,[4] wobei im Fokus, wie es der Name bereits anklingen lässt, die Innovation steht. Das gesamte Gesundheitswesen soll digitalisiert werden und die Umsetzung und umfassende Nutzung einer elektronischen Patientenakte gefördert werden. Leistungserbringer sollen vernetzt werden und Patienten einen Anspruch auf digitale Gesundheitsanwendungen haben. So soll die Anwendung von Gesundheits-Apps auf Smartphones zukünftig der Arzt bzw. die Ärztin verschreiben und die Krankenkasse genehmigen können (§ 33a Entwurf „Digitale-Versorgung-Gesetz"). Dem Bundesinstitut für Arzneimittel und Medizinprodukte soll dabei die Aufgabe übertragen werden, ein amtliches Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen zu führen.[5] Geplant ist außerdem, telemedizinische Leistungen zu stärken, wie etwa Videosprechstunden. Um dies umsetzen, ist ein entsprechendes verpflichtendes digitales Netzwerk erforderlich - die eingangs beschriebene Telematikinfrastruktur. Hieran sollen sich nicht nur Ärzte anschließen müssen, sofern sie keine Honorarkürzungen in Kauf nehmen wollen, sondern ebenso Apotheken (bis zum 30.09.2020) und Krankenhäuser (bis zum 01.01.2021).

Im Referenten-Entwurf „Digitale-Versorgung-Gesetz" mit Bearbeitungsstand vom 15.05.2019 war im Übrigen noch eine eigenständige Regelung zur elektronischen Patientenakte geplant (§ 291h SGB V Entwurf Digitale-Versorgung-Gesetz vom 15.05.2019).[6] Dieser Vorschlag wurde mit Beschluss des Bundeskabinetts vom 10.07.2019 gestrichen, so dass die bislang geltende Regelung des § 291a SGB V vorerst weiterhin Geltung beansprucht. Allerdings sollen nach Angaben des Bundesgesundheitsministeriums Regelungen zur elektronischen Patientenakte nun in einem eigenen Datenschutzgesetz erfolgen.[7] Die Datenschutz-Grundverordnung enthält insoweit eine Öffnungsklausel (Artikel 9 Absatz 4 DSGVO), die dem nationalen Gesetzgeber Regelungen zur Verarbeitung von Gesundheitsdaten ermöglicht, etwa im Rahmen des Sozialgesetzbuches V (SGB V) oder auch im Rahmen eines neuen, für die Verarbeitung von Gesundheitsdaten spezifischen Datenschutzgesetzes. Ergänzend ist in diesem Kontext zu erwähnen, dass zwar ebenso gesetzliche Regelungen im Hinblick auf die Tarifgestaltung in Verknüpfung mit erhobenen Gesundheitsdaten denkbar wären. Insgesamt wird von der Arbeitsgruppe Digitaler Neustart allerdings die Auffassung vertreten, dass eine gesetzliche Regelung, die die laufende Erhebung personenbezogener Gesundheitsdaten zu Zwecken der Tarifgestaltung in der privaten Krankenversicherung erlaubt, für unzulässig erklärt werden sollte. Begründet wird dies mit der Gefahr von möglichen Diskriminierungen, der Verknüpfungsmöglichkeit von Daten sowie eines Datendiebstahls.[8]

III. Definition von Gesundheitsdaten

Patientenbezogene Daten (z. B. Anamneseangaben, Befunde, Behandlungs-

empfehlungen) sind bekanntermaßen besonders schützenswerte Daten und unterliegen einer Verschwiegenheitsverpflichtung. Die Datenschutz-Grundverordnung enthält in Artikel 4 Nr. 15 DSGVO eine Legaldefinition für Gesundheitsdaten. Danach sind „Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Allerdings soll grundsätzlich ein weites Verständnis von Gesundheitsdaten erfolgen.[9] So sei auch die regelmäßige Ermittlung der Schrittzahl in Verbindung mit Körperdaten, wie etwa Alter, Größe, Gewicht, dazu geeignet Rückschlüsse auf den Gesundheitszustand zuzulassen, so dass durch Sportuhren oder Fitnesstracker erhobene Daten als Gesundheitsdaten einzustufen seien.[10] Allgemein ist im Hinblick auf solche so genannte Wearables, wie Fitnessarmbänder oder Smart Watches, darauf hinzuweisen, dass im Jahre 2016 sieben deutsche Aufsichtsbehörden eine deutschlandweite Prüfaktion durchführten und zu dem Ergebnis gelangten, dass kein Gerät vollständig die datenschutzrechtlichen Anforderungen erfüllte.[11] Auch im Abschlussbericht der Datenethikkommission wird darauf hingewiesen, dass die Qualität dieser Apps und damit auch die Verwertbarkeit der dadurch erhobenen Daten vielfach nicht hoch und auch nicht umfassend geprüft sei.[12] Dies berge für die betroffenen Patienten und Nutzer ein zuweilen beträchtliches Gesundheitsrisiko.[13]

Diese datenschutzrechtlichen Bedenken müssen berücksichtigt und gelöst werden, wenn die derzeitigen Planungen im Entwurf zum Digitale-Versorgung-Gesetz verwirklicht werden und ein Leistungsanspruch der Versicherten auf digitale Gesundheitsanwendungen geschaffen wird.[14]

IV. Gesetzliche Grundlagen gemäß Sozialgesetzbuch V

- Gesundheitskarte

Die Gesundheitskarte wird von den Krankenkassen für jede Versicherte und jeden Versicherten ausgestellt. Auf ihr werden die Stammdaten gespeichert (Name, Geburtsdatum, Adresse, Geschlecht, Krankenkasse und Versichertennummer). Mit Anbindung an die Telematikinfrastruktur sind Ärzte und Psychotherapeuten verpflichtet, diese mit den Daten der Krankenkassen online abzugleichen (so genannter Stammdatenabgleich).[15] Grundsätzlich dient die Gesundheitskarte der Abrechnung sowie dem Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung (Versicherungsnachweis). Gemäß § 291 Absatz 2 Satz 2 Entwurf „Digitale-Versorgung-Gesetz" soll zukünftig außerdem die Möglichkeit eröffnet werden, weitere Angaben zum Versicherten


Bild: Shutterstock

oder zum Versicherungsverhältnis auf der elektronischen Gesundheitskarte zu speichern.[16]

Ärzte, Einrichtungen und Zahnärzte sind im Übrigen verpflichtet den Anschluss an die Telematikinfrastruktur umzusetzen. Anderenfalls wird ihre Vergütung vertragsärztlicher Leistungen pauschal um 1 Prozent gekürzt (§ 291 2b SGB V). Gemäß des Referentenentwurfs „Digitale-Versorgung-Gesetz" ist zukünftig sogar eine Erhöhung der Honorarkürzung vertragsärztlicher Leistungen auf 2,5% geplant. Begründet wird dies mit der Verpflichtung der Ärzte zur Durchführung des Versichertenstammdatenmanagements, wofür der Anschluss an die Telematikinfrastruktur erforderlich sei, was wiederum Voraussetzung für die Nutzung der medizinischen Anwendungen einschließlich der elektronischen Patientenakte sei.[17] Allerdings hält der Bundesrat diese Verschärfung für nicht zielführend, da die zahlreichen Probleme mit dem Anschluss der Praxen der niedergelassenen Ärzte an die Telematikinfrastruktur oftmals nicht in der Verantwortung der Ärzte liegen würden, sondern häufig niedergelassene Ärzte in ländlichen, vom Breitbandausbau noch nicht vollständig erfassten Regionen betroffen seien.[18]

- Elektronische Patientenakte

Die Krankenkassen sind verpflichtet, ihren Versicherten spätestens ab dem 1. Januar 2021 eine elektronische Patientenakte zur Verfügung zu stellen (§ 291a Absatz 5c SGB V).[19] Zu diesem Zweck muss die Gesundheitskarte geeignet sein das Verarbeiten von medizinischen Daten im Rahmen einer elektronischen Patientenakte zu unterstützen (§ 291 Absatz 3 SGB V). Insgesamt sollen von der Gesundheitskarte Daten, soweit sie für die Notfallversorgung erforderlich sind, sowie u.a. Befunde oder Diagnosen umfasst sein. Dies stellt nach dem Willen des Gesetzgebers die Voraussetzung für ein modernes Gesundheitswesen dar: der schnelle und problemlose Zugriff auf Patientendaten.

Damit eine Vernetzung in der Praxis aber auch tatsächlich stattfinden kann, sollen nach den Plänen des Gesundheitsministeriums die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer gegenüber der jeweils zuständigen Kassenärztlichen Vereinigung nachweisen müssen, dass sie über die für den Zugriff auf die elektronische Patientenakte erforderlichen Komponenten und Dienste verfügen. Wird ein solcher Nachweis nicht bis zum 30. Juni 2021 erbracht, soll die Vergütung vertragsärztlicher Leistungen pauschal um 1 Prozent so lange gekürzt werden, bis der Nachweis gegenüber der Kassenärztlichen Vereinigung erbracht ist (§ 291 Absatz 2c Entwurf „Digitale-Versorgung-Gesetz").

- Elektronische Gesundheitsakte

Die elektronische Gesundheitsakte (§ 68 SGB V) ist von der elektronischen Patientenakte (§ 291a SGB V) zu unterscheiden. Bereits die ehemalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hatte klargestellt, dass die Zurverfügungstellung einer elektronischen Gesundheitsakte (eGA) keine gesetzliche Aufgabe sei, aber Krankenkassen die persönliche elektronische Gesundheitsakte ihrer Versicherten finanziell unterstützen können. In diesem Sinne wird ebenso im aktuellen Tätigkeitsbericht zum Datenschutz 2017-2018 des amtierenden Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ausgeführt, dass es sich bei elektronischen Gesundheitsakten um ein privates Angebot von Dritten handelt, die weder Sozialdaten verarbeiten noch das Sozialgeheimnis beachten müssen.[20] Elektronische Gesundheitsakten werden dementsprechend von einzelnen Krankenkassen ihren Versicherten als Satzungsleistung bereitgestellt und bieten unterschiedliche Funktionalitäten (Medikationsplan, Arztsuche, Terminverwaltung, Impfpass, Notfalldaten). Sie dienen dem Zweck Dokumente von Ärzten oder Laboren digital anzufragen und zu verwalten. Die Dienstleister bieten diese Funktion hauptsächlich als App für das Mobiltelefon an, um medizinische Daten (z.B. Befunde oder Laborwerte) jederzeit und an jedem Ort abrufbar und verfügbar zu gestalten. Die Telematikinfrastruktur (bereitgestellt durch die gematik) spielt hierbei aktuell noch keine Rolle. Gemäß dem Entwurf zum Digitale-Versorgung-Gesetz sollen allerdings die auf Grundlage des § 68 SGB V von den Krankenkassen finanzierten elektronischen Gesundheitsakten durch elektronische Patientenakten nach § 291a Absatz 3 Satz 1 Nr. 4 ersetzt werden und die Regelung in § 68 SGB V daher zukünftig entfallen.[21] Ab dem 1. April 2022 dürfen die elektronischen Gesundheitsakten gemäß dem Entwurf „Digitale-Versorgung-Gesetz" nicht mehr finanziert werden.

V. Herausforderungen und Kritikpunkte

- Elektronische Patientenakte

Kritisiert wird einerseits, dass Leistungserbringer (Ärzte und Ärztinnen, etc.) – wie oben bereits beschrieben – verpflichtet werden sich der Telematikinfrastruktur anzuschließen.[22] Andererseits werden Zweifel daran erhoben, ob in der Praxis das erforderliche Berechtigungsmanagement seitens der Patienten und Patientinnen bei Einführung der elektronischen Patientenakte umgesetzt werden kann. So muss die Verfügungshoheit des Patienten und der Patientin über die sensiblen Daten sichergestellt sein.[23] Entsprechend ist derzeit in § 291a Absatz 5 SGB V geregelt:

- Das Erheben, Verarbeiten und Nutzen von Daten ist nur mit dem Einverständnis der Versicherten zulässig. Soweit es zur Notfallversorgung erforderlich ist, ist der Zugriff auf Daten auch ohne eine Autorisierung der Versicherten zulässig.
- Durch technische Vorkehrungen ist zu gewährleisten, dass der Zugriff nur durch Autorisierung der Versicherten möglich ist. Der Zugriff auf Daten der Patientenakte darf grundsätzlich nur in Verbindung mit einem elektronischen Heilberufsausweis erfolgen, wenn eine Möglichkeit zur sicheren Authentifizierung und über eine qualifizierte elektronische Signatur besteht.
- Ein Zugriff der Patienten auf ihre Daten kann auch ohne Einsatz der elektronischen Gesundheitskarte erfolgen, wenn der Versicherte nach umfassender Information durch seine Krankenkasse gegenüber der Krankenkasse schriftlich oder elektronisch erklärt hat, dieses Zugriffsverfahren zu nutzen.

Ohne diese umfassende Verfügungsbefugnis würde ein Eingriff in das infor-

mationelle Selbstbestimmungsrecht des Patienten vorliegen: So wird vertreten, dass die Führung und die Anlage einer elektronischen Patientenakte stets der Einwilligung des Patienten bedarf und weder gesetzliche Erlaubnisse zur Führung einer elektronischen Patientenakte durch medizinische Leistungserbringer, welche implizit eine einseitige Duldungspflicht der Patienten beinhalten, noch beidseitige Verpflichtungen sowohl zur Führung seitens der Leistungserbringer als auch zur Duldung durch die Patienten verfassungskonform seien.[24] Es läge damit ein nicht zu rechtfertigender Eingriff in das informationelle Selbstbestimmungsrecht des Patienten vor.

Im Hinblick auf die Leistungserbringer, z.B. Ärzte, liegt mit der Verpflichtung zur Führung einer elektronischen Patientenakte (unabhängig von der Einwilligung des Patienten) zwar ebenfalls ein Eingriff in deren informationelles Selbstbestimmungsrecht vor. Allerdings wird dieser Eingriff als gerechtfertigt eingestuft, da nur Daten der Sozialsphäre betroffen sind.[25] Auch ein Eingriff in die Berufsausübungsfreiheit soll aufgrund des Schutzes der Gesundheit sowie der Förderung der informationellen Selbstbestimmung der Patienten gerechtfertigt sein.[26] Allerdings erfolgt in diesem Zusammenhang ebenso der Hinweis auf eine angemessene Vergütung des damit verbundenen Zusatzaufwands beim jeweiligen Leistungserbringer und darauf, dass weiterhin Haftungsrisiken der Ärzte durch Gesetzgebung, Verwaltung und Rechtsprechung nicht überzogen werden dürften.[27] Die Haftungsrisiken sind unter anderem darauf zurückzuführen, dass Patientendaten auf Verlangen des Patienten bzw. der Patientin wieder gelöscht werden müssen. Den Patientinnen und Patienten stehen darüber hinaus eigene Löschungsrechte zu (§ 291a Absatz 6 SGB V) zu. Dies hat aber auch zur Folge, dass nicht notwendigerweise eine medizinisch vollständige Akte vorliegt, was wiederum haftungsrechtliche Konsequenzen nach sich ziehen kann: So kann sich ein Arzt bzw. eine Ärztin nicht darauf verlassen, dass tatsächlich alle relevanten Patientendaten vorliegen, wozu ebenso Notfalldaten zählen können.[28] Daher gibt es bereits einzelne Äußerungen dahingehend, dass eine gesetzliche Verpflichtung zur Nutzung und Duldung einer Patientenakte notwendig sei, um ihre Vollständigkeit sicherzustellen. Allerdings muss an dieser Stelle wiederum auf die gerade dargestellten verfassungsrechtlichen Bedenken hingewiesen werden. Es handelt sich um einen außerordentlich sensiblen Bereich der informationellen Selbstbestimmung. So betont auch die Fraktion BÜNDNIS 90/DIE GRÜNEN die Wichtigkeit eines entsprechenden Einwilligungs- und Berechtigungsmanagements für die in die elektronischen Patientenakte einzustellenden sensiblen Gesundheitsdaten, die Gewährleistung einer freiwilligen und informierten Einwilligung etwa durch entsprechende Informationspflichten der Leistungserbringer und Krankenkassen sowie ein differenziertes gesetzliches Konzept von Zugriffsbestimmungen und Zugriffsbeschränkungen.[29] Ebenso wird dabei die Sicherung der informellen Selbstbestimmungsrechte der Patientinnen und Patienten als eine Grundvoraussetzung für Akzeptanz und Vertrauen hervorgehoben, damit die digitale Transformation überhaupt gelingen könne.[30]

- Elektronische Gesundheitsakte

Die Funktionsweise einer Gesundheitsakte kann den Ausführungen der Berliner Beauftragten für Datenschutz und Informationsfreiheit in ihrem Jahresbericht unter dem Stichwort „Problematische Einführung einer elektronischen Gesundheitsakte“ entnommen werden:[31] Danach können Versicherte mittels einer auf ihrem Mobiltelefon installierten App dem Anbieter mitteilen, dass sie Unterlagen von einer behandelnden Ärztin oder einem behandelnden Arzt erhalten möchten und der Anbieter könnte sich anschließend per E-Mail an die betreffende Ärztin oder an den betreffenden Arzt wenden, die wiederum das entsprechende Dokument über den Webbrowser in die Akte hochladen können.[32] Letztendlich handelt es sich daher um eine Kopie der vom Patienten gewünschten Daten in die elektronische Akte. Sowohl die Arztpraxis als auch Anbieter der Gesundheitsakte haben hierbei die Anforderungen von Datenschutz und Datensicherheit in ihrem jeweiligen Verantwortungsbereich sicherzustellen.

Außerdem ist zu bedenken, dass eine elektronische Gesundheitsakte als freiwillige Satzungsleistung der Krankenkassen von privaten Anbietern zur Verfügung gestellt wird. Es werden demnach private Dritte eingebunden und die Patientendaten verbleiben nicht mehr allein im geschützten Patient-Arzt-Verhältnis. Entsprechend erfolgt seitens der Berliner Beauftragten für Datenschutz und Informationsfreiheit der Hinweis, dass medizinische Leistungserbringer patientenbezogene Daten nur dann an Betreiber elektronischer Gesundheitsakten übermitteln dürfen, wenn die entsprechende Anforderung tatsächlich von der behandelten Person ausgeht.[33] Daher ist auch eine Erklärung über die Entbindung von der Schweigepflicht erforderlich.

Ergänzend ist darauf hinzuweisen, dass Anbieter von elektronischen Gesundheitsakten in der Vergangenheit in Kritik geraten sind, da ohne Einwilligung der Nutzer Analysetools genutzt wurden, die Daten etwa in Bezug auf Systemabstürze und Fehler sammelten und/oder personenbeziehbare Daten an Tracking- und Analysedienstleister übermittelten.[34] Allerdings bedarf es nach Auffassung der Datenschutzkonferenz einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, und bei der Erstellung von Nutzerprofilen. Das bedeutet – so die Datenschutzkonferenz – dass eine informierte Einwilligung i. S. d. DSGVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung, vor der Datenverarbeitung eingeholt werden muss, d. h. z.B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.[35] Beim Einsatz von Tracking- und Analysetools ist allein die Information folglich nicht ausreichend.

VI. Umsetzung in der Arztpraxis

- Datenschutzrechtliche Anforderungen

Mit Blick auf die elektronische Patientenakte, die elektronische Gesundheitsakte und die elektronische Gesundheitskarte müssen die Ärztinnen und Ärzte in ihrem Verantwortungsbereich „Arztpraxis“ ebenso Pflichten der Datenschutz-Grundverordnung umset-

zen. Patientendaten dürfen grundsätzlich etwa aufgrund der oben genannten Regelungen des SGB V, aufgrund der Erforderlichkeit im Rahmen des Behandlungsvertrages oder aufgrund Einwilligung des Patienten verarbeitet werden. Die zuletzt genannte Rechtsgrundlage kann bei zusätzlichen Diensten in Betracht kommen, wie beispielsweise die turnusmäßige Benachrichtigung der Patienten über die Fälligkeit eines Kontrolltermins. Entsprechendes gilt für die Weitergabe der Daten von Privatpatienten an die privatärztliche Verrechnungsstelle oder eine andere private Verrechnungsstelle: Eine solche Übermittlung bedarf einer Einwilligung bzw. der Entbindung von der Schweigepflicht. Zwar ist nicht notwendigerweise eine Schriftform erforderlich,[36] dennoch ist an die Dokumentations- bzw. Nachweispflicht im Sinne der DSGVO zu denken (Artikel 5 Absatz 2 DSGVO).[37]

In einer Arztpraxis ist gleichermaßen die Transparenz der Datenverarbeitung sicherzustellen, die von der Datenschutz-Grundverordnung besonders hervorgehoben wird: Die Datenverarbeitung muss für die betroffene Person nachvollziehbar sein. Hierbei spielt das Recht auf Information gemäß Artikel 13 DSGVO eine zentrale Rolle, da es den Patienten überhaupt erst ermöglicht, ihre Rechte wahrnehmen zu können.[38] Daher gilt auch im Falle einer gesetzlichen Verpflichtung, etwa bei der Durchführung des Stammdatenabgleichs (§ 291 SGB V), dass der Arzt bzw. die Ärztin unter anderem über die Rechtsgrundlage und über die Empfänger der Daten (Krankenkassen) informieren muss. Entsprechend müssen die Informationspflichten im Rahmen der elektronischen Gesundheitsakte erfüllt werden. Rechtsgrundlage für die Weitergabe der Daten an die jeweiligen Anbieter stellt hier die informierte Einwilligung der Patienten dar. Lediglich im Hinblick auf die (anschließende) Datenverarbeitung beim Empfänger besteht keine Informations- oder Auskunftsverpflichtung. Die Information hierüber obliegt vielmehr den Krankenkassen oder aber den Anbietern elektronischer Gesundheitsakten als Empfänger der Daten.

Weiterhin muss die behandelnde Ärztin bzw. der behandelnde Arzt ein Verzeichnis von Verarbeitungstätigkeiten anlegen (Artikel 30 DSGVO). Werden beispielsweise Daten in eine elektronische Akte übermittelt, muss dieser Vorgang im Verzeichnis von Verarbeitungstätigkeiten ergänzt werden.

Die Datenschutz-Grundverordnung sieht außerdem das Instrument der so genannten Datenschutz-Folgenabschätzung für besonders riskante Verfahren vor (als Nachfolgeregelung der im BDSG-alt geregelten Vorabkontrolle). Bei einer umfangreichen Verarbeitung von Patientendaten kann unterstellt werden, dass zumindest der Anbieter des Dienstes eine solche durchführen muss. So haben die Aufsichtsbehörden als Beispiel für eine Verarbeitungstätigkeit, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, den „Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten und die zentrale Speicherung der Daten“ aufgelistet.[39] Kritisiert wird allerdings, dass die Telematikinfrastruktur ohne jegliche datenschutzrechtliche Vorab-Prüfung ausgerollt und bereits als erste Anwendung der Versichertenstammdatenabgleich in Betrieb genommen wurde.[40]

Die Datenverarbeitung in einer kleinen oder mittelgroßen Arztpraxis erfordert dagegen regelmäßig keine Datenschutz-Folgenabschätzung.[41] Da allerdings sensible Daten an Krankenkassen oder Anbieter von elektronischen Gesundheitsakten übermittelt werden, empfiehlt sich die Dokumentation seitens der Ärztin bzw. des Arztes, aus welchem Grund keine Datenschutz-Folgenabschätzung durchzuführen ist bzw. warum kein besonderes Risiko für den Patienten vorliegt („Schwellenwertanalyse“). In diesem Zusammenhang könnte etwa dokumentiert werden, dass die Daten vor deren Versendung verschlüsselt werden (siehe hierzu auch den nachfolgenden Punkt „Datensicherheit“).

Aus datenschutzrechtlicher Sicht ist im Übrigen klarzustellen, dass der Anspruch auf eine elektronische Kopie gemäß Artikel 15 Absatz 4 DSGVO nicht dazu führt, dass ein Arzt bzw. eine Ärztin zur Nutzung einer elektronischen Gesundheitsakte verpflichtet wäre. Die Nutzung kann zwar grundsätzlich die Beauskunftung erleichtern, da jeder Verantwortliche die Frist von einem Monat nach Eingang des Antrags beachten muss und eine Fristverlängerung von weiteren zwei Monaten nur im Ausnahmefall in Betracht kommt. In Bezug auf die elektronische Gesundheitsakte bedeutet dies jedoch nicht, dass ein Zwang bestehen würde, Patientendaten in eine solche einzutragen und zu übermitteln, um elektronischen Anfragen nachzukommen. Dies hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit hervorgehoben und ausgeführt, dass die Leistungserbringer grundsätzlich den Weg zur Übermittlung der elektronischen Kopie selbst wählen könnten (auch wenn ein Recht auf Erhalt einer elektronischen Kopie bestehe).[42]

- Datensicherheit

Ein Arzt bzw. eine Ärztin ist ebenso für die Datensicherheit des Praxisverwaltungssystems verantwortlich. Gemäß den Ausführungen der Berliner Beauftragten für Datenschutz und Informationsfreiheit sollten unverschlüsselte patientenbezogene Daten nicht auf Arbeitsplatzrechnern verarbeitet werden, die ungehindert auf das Internet zugreifen können, so dass patientenbezogene Daten vom Leistungserbringer vor der Übermittlung zu verschlüsseln sind. Speziell für Gesundheitsakten hat sie ausgeführt, dass die Datensicherheit sowohl vom Betreiber der elektronischen Gesundheitsakte als auch vom medizinischen Leistungserbringer gewährleistet werden muss.[43] Nach ihrer Auffassung habe der Leistungserbringer dafür Sorge zu tragen, dass die Verschlüsselung nur mit dem von der behandelten Person zur Verfügung gestellten Schlüssel erfolgt, und er muss die Verwendung des richtigen Schlüssels im Zweifelsfall nachweisen können.[44] Diese Verpflichtung ist in Artikel 32 DSGVO geregelt und verlangt vom Verantwortlichen „geeignete technische und organisatorische Maßnahmen: z.B. Pseudonymisierung und Verschlüsselung personenbezogener Daten“.

Dies entspricht im Übrigen ebenso der Auffassung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, der bereits unter altem Recht dargelegt hat, dass die *„Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthalten, ein ungeeignetes Kommunikationsmittel*

darstellt, insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen".[45] In seinem Tätigkeitsbericht aus dem Jahre 2014/2015 weist er darauf hin, dass bei der Nutzung von elektronischen Kommunikationswegen eine Verschlüsselung dringend geboten sei, insbesondere wenn es sich wie vorliegend um Gesundheits- und Sozialdaten der Betroffenen handelt.[46] In diesem Sinne hat gleichermaßen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Sozialversicherungsträger (Kranken- und Pflegekassen, Berufsgenossenschaften, Deutsche Rentenversicherung) angewiesen, mit ihren Versicherten nur auf sicherem Weg zu kommunizieren und Gesundheitsdaten ausschließlich geschützt zu versenden oder zu empfangen.[47] Unter Verweis auf das mangelhafte Sicherheitsniveau, das mit einer Postkarte vergleichbar sei, wäre nur eine verschlüsselte Versendung von Gesundheitsdaten per E-Mail mit einer qualifizierten Signatur datenschutzrechtlich zulässig.[48]

VII. Besondere Fragestellungen

- Zertifikate

Gemäß dem Kurzpapier Nr. 9 der Datenschutzkonferenz „Zertifizierung nach Artikel 42 DS-GVO" arbeiten die Aufsichtsbehörden des Bundes und der Länder derzeit intensiv an der Entwicklung abgestimmter, länderübergreifend geltender Kriterien, um einen „Wildwuchs" zahlreicher unterschiedlicher Zertifizierungsverfahren – so die Datenschutzkonferenz – gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten zu vermeiden.[49] Die Voraussetzungen für eine Zertifizierung gemäß Artikel 42 DSGVO müssen somit erst erarbeitet werden. Derzeit bestehende Zertifikate werden beispielsweise vom TÜV ausgestellt. In diesem Zusammenhang soll beispielhaft auf den Anbieter einer elektronischen Gesundheitsakte verwiesen werden, der in der Vergangenheit in seiner Produktanpreisung folgendes angab: *„vom TÜV Rheinland getestet und als sichere Plattform zertifiziert"*. Als dennoch Sicherheitsprobleme aufgedeckt und veröffentlicht wurden, stellte der TÜV Rheinland in einer Pressemitteilung klar, dass die angesprochenen Schwachstellen nicht den von ihm zertifizierten Teil der verschlüsselten Datenübertragung innerhalb der mobilen Applikation betreffen würden.[50] Insgesamt hat der TÜV (nur) konstatiert, dass die TLS-Verbindung, die zum Server des Anbieters der Gesundheitsakte aufgebaut wird, nach dem Stand der Technik gesichert sei und die damit verbundene Zertifikatsprüfung korrekt durchgeführt wurde.[51] Daher ist stets die Frage zu berücksichtigen und besonderes Augenmerk darauf zu legen: „Was bzw. welches Detail wurde zertifiziert und getestet?", um die notwendige Transparenz für die Patienten und Patientinnen sicherzustellen.

Um mehr Transparenz und Vertrauen zu schaffen, wäre es ebenso möglich, die Patientinnen und Patienten bei ihrer Auswahl zu unterstützen. Ein solcher Vorschlag kommt von der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN und zielt darauf ab, dass die Bundesregierung den Aufbau und Betrieb eines gemeinnützigen Online-Verzeichnisses mit staatlichen Mitteln unterstützt oder alternativ selbst ein Online-Verzeichnis schafft.[52]

- Forschungszwecke

Besonderer Aufmerksamkeit bedürfen die Forschung auf der Grundlage von Patientendaten und der in diesem Zusammenhang notwendige Schutz. Vielfach wird man nun den Einwand hören: „Ja, aber die Daten sind doch anonym! Dann darf man diese doch beliebig nutzen." Es ist richtig, dass anonyme Daten nicht den strengen Regeln des Datenschutzes unterfallen, da sie nur unter unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft einen Rückschluss auf die einzelne Person bzw. den Patienten erlauben. So verweisen beispielsweise Christl/Spiekermann in ihrem Buch „Networks of Control" auf viele einfache Methoden, um die Re-Identifikation herzustellen.[53] Das Zusatzwissen durch die Vernetzung und damit vereinfachter Zugriff und Verbindung mit anderen Informationen ist nicht zu unterschätzen. Daher stellt sich die Frage, ob es überhaupt noch anonyme Daten gibt. Es muss also stets die Methode der Anonymisierung hinterfragt werden.[54] Allein eine Aussage eines Anbieters dahingehend, dass selbstverständlich nur aggregierte und nicht identifizierbare Daten an Dritte weitergegeben oder für „andere" und „weitere" Zwecke genutzt werden, ist noch nicht aussagekräftig im Hinblick auf die Methode, wie von Christl/Spiekermann ebenfalls hervorgehoben wird. Auch die Aufsichtsbehörden verweisen in der Orientierungshilfe Cloud-Computing darauf, dass jede Anonymisierung einem Zeitablauf unterliegt und neu geprüft werden muss.[55] Berücksichtigt werden muss vor allem, ob eine Verschlüsselung nach dem Stand der Technik verwandt wurde bzw. ob der eingesetzte Algorithmus durch Zeitablauf keinen angemessenen Schutz mehr bietet und inwieweit ein starker oder schwacher Kryptoalgorithmus zum Einsatz kommt und anhand einer Risikoabschätzung ist die Wahrscheinlichkeit zu prüfen, den Personenbezug herzustellen.[56] Diese Analyse muss regelmäßig durchgeführt werden.[57] Diese Vorsicht ist umso mehr geboten, da gemäß Artikel 89 DSGVO grundsätzlich eine Datenverarbeitung zu wissenschaftlichen Forschungszwecken erlaubt, aber wissenschaftliche Forschung nicht notwendigerweise an einen akademischen Wissenschaftsbetrieb geknüpft ist. Außerdem sind im Sinne von § 27 Absatz 3 BDSG Gesundheitsdaten, die zu wissenschaftlichen Forschungszwecken verarbeitet werden, grundsätzlich erst zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Die Datenethikkommission schlägt als weitere Schutzmaßnahme strafbewehrte Verbote einer De-anonymisierung vor (für den Fall, dass bei bisher anonymen Daten, etwa durch die Entwicklung der Technik, ein Personenbezug hergestellt werden kann).[58]

Im Entwurf zum „Digitale-Versorgung-Gesetz" wird unter dem Punkt „Die Regelungen zur Datentransparenz werden weiterentwickelt" betont, dass die Sozialdaten der Krankenkassen eine wertvolle Datenquelle nicht nur für die Steuerung und Weiterentwicklung der Gesundheitsversorgung in der gesetz-

lichen Krankenversicherung, sondern auch für die wissenschaftliche Forschung sind.[59] Daher soll der Zugang zu den Sozialdaten verbessert werden, um eine breite wissenschaftliche Nutzung unter Wahrung des Sozialdatenschutzes zu ermöglichen und zu diesem Zwecke die bisherige Datenaufbereitungsstelle zu einem Forschungsdatenzentrum mit einem deutlich erweiterten und aktuelleren Datenangebot weiterentwickelt werden.[60] Der Bundesrat unterstützt diese Privilegierung der Forschungsdatennutzung und bittet zudem, im Gesetzgebungsverfahren zu prüfen, ob der vorliegende Vorschlag zur Etablierung eines Forschungsdatenzentrums dahingehend weiterentwickelt werden kann, dass zur Förderung der Patientensicherheit und qualitativen Weiterentwicklung digitaler Innovationen, die Daten grundsätzlich faktisch anonymisiert auch gegenüber den Herstellern zugänglich gemacht werden.[61] Außerdem schlägt der Bundesrat vor, im weiteren Gesetzgebungsverfahren bereits existierende themenspezifische Forschungsdatenbanken von nationaler und internationaler Bedeutung zu berücksichtigen und ihre Weiterführung durch wissenschaftliche Einrichtungen sicherzustellen, z.B. durch Regelungen, die es ermöglichen, pseudonymisierte Daten öffentlich grundfinanzierten Einrichtungen zu übermitteln, wenn der angegebene Zweck eine solche Übermittlung erfordert.[62] Diesen Vorschlägen ist also insgesamt zu entnehmen, dass die Verarbeitung von Daten zu Forschungszwecken ausgeweitet werden soll. Auch die Datenethikkommission sieht in einer Datennutzung für gemeinwohlorientierte Forschungszwecke (z. B. zur Verbesserung der Gesundheitsfürsorge) enormes Potenzial, das es zum Wohle des Einzelnen und der Allgemeinheit zu nutzen gilt.[63] Allerdings sollte unter Berücksichtigung des informationellen Selbstbestimmungsrechts stets die Entscheidungsfreiheit der Patientinnen und Patienten im Mittelpunkt stehen. Hierfür ist Transparenz und Vertrauen notwendig. So schlägt die Fraktion BÜNDNIS 90/DIE GRÜNEN etwa vor, einen Rechtsrahmen zu schaffen, durch den die Patientinnen und Patienten die Möglichkeit erhalten, ihre Gesundheitsdaten in pseudonymisierter Form freiwillig, widerrufbar und wenn gewünscht auch zweckgebunden für einzelne Vorhaben der Forschung zur Verfügung zu stellen und entsprechende Nutzungsrechte einzuräumen.[64] Betont wird hierbei eine in Abstimmung mit den Datenschutzbehörden zu erarbeitende, den europarechtlichen Vorgaben der DSGVO entsprechende Einwilligungslösung.[65] Die Datenethikkommission empfiehlt bei der Forschung mit besonders sensiblen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten), die Forschenden durch Handreichungen zur rechtssicheren Einholung von Einwilligungen sowie durch die Förderung und gesetzliche Anerkennung innovativer Einwilligungsmodelle zu unterstützen.[66] Dazu könnten nach Auffassung der Datenethikkommission auch digitale Einwilligungsassistenten gehören.

Auch im Rahmen von Forschungszwecken kommt der informationellen Selbstbestimmung also eine besondere Bedeutung zu, die im weiteren Gesetzgebungsverfahren berücksichtigt werden muss.

VII. Fazit

Unbestritten ist die Wichtigkeit der Digitalisierung – insbesondere unter dem Aspekt der verbesserungswürdigen medizinischen Versorgung in ländlichen Gebieten. Auch die Datenethikkommission spricht sich mit Blick auf die Vorteile eines digitalisierten Gesundheitswesens für einen raschen Ausbau digitaler Infrastrukturen innerhalb des Gesundheitssektors aus. Der qualitative und quantitative Ausbau digitalisierter Versorgungsmaßnahmen sollte – so die Ausführungen der Datenethikkommission – die informationelle Selbstbestimmung des Patienten stärken.[67] Letztendlich ist zu berücksichtigen, dass sehr sensible Daten im Fokus stehen und eine Vernetzung von Daten für die Betroffenen gleichermaßen mit Gefahren verbunden sein kann: Durch unsicher konfigurierte Server können (Millionen von) Daten geleakt werden,[68] außerdem werden sich Hackerangriffe nicht vermeiden lassen und Gesundheits-Apps auf einem Smartphone beinhalten ebenso Sicherheitsrisiken. Ein Anbieter einer elektronischen Gesundheitsakte hat in der Vergangenheit sogar die Empfehlung ausgesprochen, aus Sicherheitsgründen keine gerooteten Geräte, wie ein Android-Endgerät zu verwenden, da dadurch die Datensicherheit der von ihm zur Verfügung gestellten App nicht mehr gegeben sei. Eine wesentliche Anforderung ist daher die Sicherstellung einer umfassenden Transparenz als Entscheidungsgrundlage für das informationelle Selbstbestimmungsrecht. Hierfür sind wiederum Praktikabilität und Verständlichkeit der jeweiligen Anwendung eine wichtige Voraussetzung. Dies wird auch als digitale Souveränität bezeichnet: Patientinnen und Patienten müssen über ihre Daten im Sinne einer digitalen Souveränität bestimmen können. Andererseits ist ebenso eine digitale Ethik unerlässlich. Die Datenethikkommission empfiehlt, bereits bei der Entwicklung der elektronischen Patientenakte die Vielfalt ethischer Aspekte als integralen Bestandteil im Rahmen eines „ethics by, in and for design"-Ansatzes zu berücksichtigen.[69] Sarah Spiekermann formuliert diese Anforderung weitaus anschaulicher: „Wir brauchen eine Technik, die uns dient anstatt uns zu beherrschen. Man braucht einen nüchternen Verstand in der Abschätzung dessen, was das Digitale kann und was nicht – wo es guttut und wo es schädlich ist."[70]

Es geht also nicht nur darum, dass Unternehmen (glaubwürdig) ethische Maßstäbe in ihre Unternehmenspolitik integrieren, sondern wir haben eine gesamtgesellschaftliche Aufgabe. Zudem zeigt sich gerade bei Patientendaten, wie wichtig es ist, ethische Grundsätze bereits im Gesetzgebungsverfahren mitzudenken und die Richtung vorzugeben. Die Hoffnung ist also, dass wir alle diese Besonnenheit zukünftig umsetzen können – damit uns die Digitalisierung nutzt und nicht schadet.

1 Siehe Heise „Kritiker dieser Monsterdatei gehen davon aus, dass die Daten über den Zugang zur „Forschung" sehr schnell ihren Weg zur Pharma-Industrie finden werden. Denn bekanntlich finanzieren Firmen einen Großteil der medizinischen Forschung. Eine alle Patienten umfassende bundesweite zentrale Datensammlung würde sicherlich auch ein begehrtes Ziel von allerlei kriminellen Begierden.", abrufbar unter https://www.heise.de/tp/features/Wer-braucht-die-zentrale-Patientendatei-4223472.html.

2 Im Einzelnen: Bundesministerium für Gesundheit (BMG), die Bundesärztekammer (BÄK), die Bundeszahnärztekammer (BZÄK), der Deutsche Apothekerverband (DAV), die Deutsche Krankenhausgesellschaft (DKG), der Spitzenverband der Gesetzlichen Krankenversicherungen (GKV-SV), die Kassenärztliche Bundesvereinigung (KBV) und die Kassenzahnärztliche Bundesvereinigung (KZBV), siehe unter https://www.gematik.de/ueber-uns/unternehmensstruktur/.

3 Gesetz vom 06.05.2019 BGBl. I S. 646 (Nr. 18).

4 Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale Versorgung-Gesetz – DVG) vom 23.09.2019, abrufbar unter: http://dip21.bundestag.de/dip21/btd/19/134/1913438.pdf. Der Bundestag hat am 27.09.2019 diesen Entwurf der Bundesregierung in erster Lesung beraten. Dieser wurde sodann gemeinsam mit dem Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN („Der Digitalisierung im Gesundheitswesen eine Richtung geben – Den digitalen Wandel im Interesse der Nutzerinnen und Nutzern vorantreiben") zur federführenden Beratung an den Gesundheitsausschuss überwiesen, abrufbar unter: http://dip21.bundestag.de/dip21/btd/19/135/1913539.pdf. Die Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates ist abrufbar unter: http://dip21.bundestag.de/dip21/btd/19/135/1913548.pdf. Am 16.10.2019 fand über den Gesetzentwurf eine öffentliche Anhörung des Gesundheitsausschusses unter Einbindung von Experten statt (https://www.bundestag.de/dokumente/textarchiv/2019/kw42-pa-gesundheit-dvg-660398. Der frühere Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale Versorgung-Gesetz – DVG) vom 10.07.2019, ist abrufbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/Digitale-Versorgung-Gesetz_DVG_Kabinett.pdf .
Anmerkung der Redaktion:
Das Digitale-Versorgung-Gesetz wurde am 07.11.2019 vom Bundestag beschlossen: https://www.bundestag.de/dokumente/textarchiv/2019/kw45-de-digitale-versorgung-gesetz-664900. Am 29.11.2019 hat der Bundesrat das Digitale-Versorgung-Gesetz gebilligt: https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2019/0501-0600/0557-19.html.
Das Gesetz wird über die Bundesregierung dem Bundespräsidenten zur Unterzeichnung zugeleitet. Es soll am Tag nach der Verkündung im Bundesgesetzblatt in Kraft treten.

5 Siehe S. 35 im Entwurf des „Digitale-Versorgung-Gesetz" vom 23.09.2019 (Endnote 4): „Dem Bundesinstitut für Arzneimittel und Medizinprodukte wird die Aufgabe übertragen, ein amtliches Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen zu führen und auf Antrag der Hersteller über die Aufnahme zu entscheiden. Voraussetzung für eine Aufnahme ist neben der Erfüllung der Anforderungen an Sicherheit, Funktionstauglichkeit, Qualität, Datenschutz und Datensicherheit insbesondere der Nachweis positiver Versorgungseffekte durch den Hersteller."

6 Siehe Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz), Bearbeitungsstand: 15.05.2019, abrufbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/Digitale_Versorgung_Gesetz_-_RefEntwurf.pdf.

7 Davon soll jedoch die Einführung der elektronischen Patientenakte zum 01.01.2021 unberührt bleiben. Siehe hierzu die Informationen auf der Webseite des Bundesgesundheitsministeriums, abrufbar unter https://www.bundesgesundheitsministerium.de/digitale-versorgung-gesetz.html.

8 Eine entsprechende Regelung wäre im Versicherungsvertragsgesetz (VVG) möglich, siehe Arbeitsgruppe „Digitaler Neustart", der Konferenz der Justizministerinnen und Justizminister der Länder, Bericht vom 01.10.2018 „Gesundheitsdaten", S. 119 ff. (124).

9 Siehe Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder, Bericht vom 01.10.2018 „Gesundheitsdaten", S. 106 mit Verweis in Fußnote 334 auf Dregelies, Max, Wohin laufen meine Daten? – Datenschutz bei Sportuhren und Fitnesstrackern, VuR 2017, 256 (258/259).

10 Siehe Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder, Endnote 9.

11 Siehe hierzu die Informationen des Hessischen Datenschutzbeauftragten, Datenschutzbehörden prüfen Wearables, Stand: 05.12.2016, abrufbar unter: https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/datenschutzbeh%C3%B6rden-pr%C3%BCfen-wearables.

12 Siehe Gutachten der Datenethikkommission, S. 114, veröffentlicht am 23.10.2019, abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf.

13 Siehe Gutachten der Datenethikkommission, aaO.

14 Gemäß der Gesetzesbegründung des Entwurfes des „Digitale-Versorgung-Gesetz" vom 23.09.2019 eröffnen digitale Gesundheitsanwendungen vielfältige Möglichkeiten und es soll – wie oben bereits dargestellt – ein Leistungsanspruch der Versicherten auf digitale Gesundheitsanwendungen geschaffen werden, der u.a. Software und „Gesundheits-Apps" umfasst, wie sie etwa im Rahmen von elektronischen Gesundheitsakten verwendet werden.

15 Die an der vertragsärztlichen Versorgung teilnehmenden Ärzte sind bei der erstmaligen Inanspruchnahme ihrer Leistungen durch einen Versicherten im Quartal verpflichtet, die Leistungspflicht der Krankenkasse zu prüfen. Zu diesem Zweck wird ein Stammdatenabgleich durchgeführt und geprüft, ob die auf der Gesundheitskarte des Patienten gespeicherten Daten gültig und aktuell sind. Der Referentenentwurf „Digitale-Versorgung-Gesetz" sieht vor, dass Leistungserbringer ohne unmittelbaren Patientenkontakt, beispielsweise Labore, vom Stammdatenabgleich befreit sind. Diese sollen dennoch bis zum 30.06.2020 verpflichtet sein, sich an die Telematikinfrastruktur anzuschließen.

16 Siehe Gesetzesbegründung im Entwurf „Digitale-Versorgung-Gesetz" vom 23.09.2019, S. 65 (Endnote 4).

17 Siehe Gesetzesbegründung im Entwurf „Digitale-Versorgung-Gesetz" vom 23.09.2019, S. 66 (Endnote 4).

18 Siehe Stellungnahme des Bundesrates im Entwurf „Digitale Versorgung-Gesetz" vom 23.09.2019, S. 92 (Endnote 4).

19 Gemäß § 291 Absatz 2a SGB V sind die Krankenkassen außerdem verpflichtet, Versicherten ab dem 1. Dezember 2019 auf Verlangen unverzüglich eine elektronische Gesundheitskarte mit kontaktloser Schnittstelle zur Verfügung zu stellen.

20 Siehe auch 27. Tätigkeitsbericht zum Datenschutz 2017-2018 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Bereich „Elektronische Gesundheits- und Patientenakten sowie sog. GesundheitsApps", S. 57, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/27TB_17_18.pdf.

21 Siehe S. 46 im Entwurf „Digitale-Versorgung-Gesetz" vom 23.09.2019 (Endnote 4).

22 Siehe Endnote 1.

23 Siehe Antrag der Fraktion BÜNDNIS90/DIE GRÜNEN, abrufbar unter: http://dip21.bundestag.de/dip21/btd/19/135/1913539.pdf. Hier ist folgende Anmerkung zu finden: „Parlamentarische Anfragen zeigen, dass das Bundesministerium für Gesundheit bereits seit April 2018 Kenntnis von dem fehlenden Berechtigungsmanagement hat", und zwar unter Verweis auf: https://www.aerzteblatt.de/nachrichten/105916/.

24 Schneider, Einrichtungsübergreifende elektronische Patientenakten, Zwischen Datenschutz und Gesundheit, S. 526.

25 Schneider, Einrichtungsübergreifende elektronische Patientenakten, Zwischen Datenschutz und Gesundheit, S. 527.

26 Schneider, aaO, S. 527.

27 Schneider, aaO, S. 527.

28 Haftungsrechtliche Fragen sind im Bürgerlichen Gesetzbuch geregelt (§ 630h BGB).

29 Siehe Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, abrufbar unter http://dip21.bundestag.de/dip21/btd/19/135/1913539.pdf.

30 Siehe Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, aaO.

31 Siehe Kapitel 6.3. „Problematische Einführung einer elektronischen Gesundheitsakte", S. 98, im Jahresbericht 2018 der Berliner Beauftragten für Datenschutz und Informationsfreiheit, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2018-Web.pdf.

32 Siehe Jahresbericht 2018 der Berliner Beauftragten für Datenschutz und Informationsfreiheit, aaO.

33 Siehe Jahresbericht der Berliner Beauftragte für Datenschutz und Informationsfreiheit, aaO.

34 Siehe etwa den Bericht unter https://www.heise.de/ct/artikel/Massive-Datenschutzmaengel-in-der-Gesundheits-App-Ada-4549354.html.

35 Siehe Positionsbestimmung der der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018, https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Konferenzen/Nationale_Datenschutzkonferenz/Unterlagen_der_DSK/95._Konferenz/Positionsbestimmung-TMG.pdf vom 26. April 2018 sowie Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf (März 2019). Eine entsprechende Planung ist im Übrigen dem Vorschlag der ePrivacy-Verordnung zu entnehmen (Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010. Einen Überblick zum derzeitigen Verhandlungsstand der ePrivacy-Verordnung stellt der bayerische Landesbeauftragte für den Datenschutz zur Verfügung, abrufbar unter: https://www.datenschutz-bayern.de/0/eprivacyVO.html.

36 Eine gesetzliche Ausnahme war in § 73 SGB 1b) SGB V a.F. (in der vor dem 11.05.2019 geltenden Fassung des SGB V) geregelt. Danach durfte ein Hausarzt nur mit schriftlicher Einwilligung des Versicherten bei Leistungserbringern, die einen seiner Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Auch umgekehrt durften die behandelten Leistungserbringer dem Hausarzt nur mit schriftlicher Einwilligung des Versicherten die Behandlungsdaten zum Zwecke der bei diesem durchzuführenden Dokumentation und der weiteren Behandlung übermitteln. Die Neuregelung (in der am 11.05.2019 geltenden Fassung durch Artikel 1 Gesetz vom 06.05.2019 BGBl. I S. 646) sieht lediglich vor, dass die Leistungserbringer verpflichtet sind, die den Versicherten betreffenden Behandlungsdaten und Befunde mit dessen Zustimmung zum Zwecke der bei dem Hausarzt durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln.

37 Zu betonen ist, dass eine Einwilligung stets freiwillig sein muss und die Informationspflichten erfüllt sein müssen, sowohl hinsichtlich der Widerrufsmöglichkeit als auch hinsichtlich der Identität des Empfängers, des Zwecks und des Umfangs der beabsichtigten Datenübermittlung.

38 Zu Datenschutz und Datenverarbeitung in der Arztpraxis grundsätzlich: https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Bekanntmachung_Datenschutz-Check_09.03.2018.pdf.

39 Die Aufsichtsbehörden haben eine Positivliste für Fälle erarbeitet, für welche auf jeden Fall eine Datenschutz-Folgenabschätzung erforderlich ist, abrufbar unter https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf (Liste der Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung durchzuführen ist).

40 Siehe https://patientenrechte-datenschutz.de/2019/08/21/spahns-gesundheitsnetz-als-verantwortungsfreie-zone/.

41 Siehe Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, „Die Datenschutz-Grundverordnung tritt in Kraft – das müssen selbstständige Heilberufler beachten", abrufbar unter: https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbststaendige-Heilberufler-beachten.html. In dem Papier wird außerdem darauf verwiesen, dass in besonders gelagerten Fällen etwas anderes gilt (wie bei der Benennung von betrieblichen Datenschutzbeauftragten), und zwar in den Fällen, in denen der Umfang der Verarbeitung von Gesundheitsdaten (oder anderen sensiblen Daten wie z.B. genetischen Daten) weit über das hinausgeht, was in einer üblichen Arztpraxis anzutreffen ist.

42 Siehe Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 13.12.2018, abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2018/20181213-PM-Elektronische_Gesundheitsakte.pdf.

43 Siehe Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 13.12.2018, aaO.

44 Siehe Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 13.12.2018, aaO.

45 Siehe Schreiben des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, abrufbar unter https://www.datenschutzbeauftragter-info.de/wp-content/uploads/2018/02/schreiben-der-aufsichtsbehoerde.pdf.

46 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Tätigkeitsbericht 2014/2015, S. 33, abrufbar unter: https://datenschutz-hamburg.de/assets/pdf/25._Taetigkeitsbericht_Datenschutz_2014-2015_HmbBfDI_01.pdf.

47 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, abrufbar unter https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/2019/KommunikationKrankenkassen.html.

48 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, aaO.

49 Siehe Kurzpapier Nr. 9 der Datenschutzkonferenz, abrufbar unter https://www.lda.bayern.de/media/dsk_kpnr_9_zertifizierung.pdf.

50 Siehe TÜV Rheinland: Stellungnahme zur Berichterstattung über die Sicherheit von Vivy-App vom 31.10.2018, abrufbar unter: https://www.tuv.com/de/deutschland/ueber_uns/presse/meldungen/newspdfde_410304.jsp.

51 Siehe TÜV Rheinland, aaO.

52 Siehe Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, abrufbar unter http://dip21.bundestag.de/dip21/btd/19/135/1913539.pdf.

53 Christl/Spiekermann, Networks of Control, A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy, S. 21 ff.

54 Die Autoren Christl/Spiekermann (aaO S. 22) verweisen u.a. auf eine bereits aus dem Jahre 1990 stammende Studie, in welcher festgestellt wurde, dass allein durch die Kombination durch Postleitzahl, Geschlecht und Geburtstag eine Reidentifizierung in 87% der Fälle möglich ist.

55 Siehe hierzu bereits die Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises aus dem Jahre 2014, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20141009_oh_cloud_computing.pdf.

56 Orientierungshilfe – Cloud Computing, aaO.

57 Orientierungshilfe – Cloud Computing, aaO.

58 Siehe Endnote 12 zum Gutachten der Datenethikkommission, S. 140.

59 Siehe S. 39 des Entwurfs „Digitale-Versorgung-Gesetz" vom 23.09.2019, Endnote 4.

60 Siehe S. 39 des Entwurfs „Digitale-Versorgung-Gesetz" vom 23.09.2019, Endnote 4.

61 Siehe Stellungnahme des Bundesrates zum Entwurf „Digitale-Versorgung-Gesetz" vom 23.09.2019, S. 98, Endnote 4.

62 Siehe Stellungnahme des Bundesrates zum Entwurf Digitale-Versorgung-Gesetz" vom 23.09.2019, S. 94, Endnote 4. Gemäß der Ausführungen des Bundesrates sollten hierbei aus datenschutzrechtlichen Gründen pseudonymisierte Daten nur zur Fortführung bereits existierender Langzeitdatenbanken übermittelt werden dürfen, die durch Datenübermittlung gemäß § 75 SGB X aufgebaut wurden und eine entsprechende Prüfung durchlaufen haben. Der Bundesrat fordert weiterhin, im weiteren Gesetzgebungsverfahren auf eine Löschung der versichertenbezogenen Einzeldatensätze nach 30 Jahren in begründeten Fällen zu verzichten.

63 Siehe Endnote 12 zum Gutachten der Datenethikkommission, S. 139.

64 Siehe Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, abrufbar unter http://dip21.bundestag.de/dip21/btd/19/135/1913539.pdf.

65 Siehe Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, aaO.

66 Siehe Gutachten der Datenethikkommission, S. 139.

67 Siehe Endnote 12 zum Gutachten der Datenethikkommission, S. 122. Die Datenethikkommission betont gleichermaßen, dass zum Ausbau der partizipative Auf- und Ausbau der elektronischen Patientenakte (ePa) sowie die Weiterentwicklung von Verfahren zur Prüfung und Bewertung digitaler Gesundheitsanwendungen im ersten und zweiten Gesundheitsmarkt gehöre.

68 Siehe https://www.heise.de/newsticker/meldung/Unsicher-konfigurierte-Server-leaken-Daten-von-Millionen-Patienten-4531255.html.

69 Siehe Empfehlung der Datenethikkommission für eine partizipative Entwicklung der elektronischen Patientenakte (ePA) vom 28.11.2018, abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Empfehlungen_ePA.pdf.

70 Spiekermann, Digitale Ethik: Ein Wertesystem für das 21. Jahrhundert, April 2019. Siehe auch ihre Aussage: „...wie wir auf allen Ebenen der Gesellschaft besser und weiser mit dem Digitalen umgehen sollten."

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Kritik an StPO-Änderungen zu DNA-Analysen

Das Bundeskabinett bestätigte am 23.10.2019 eine Novelle zur Strafprozessordnung (StPO), die von Bürgerrechts- und Anwaltsorganisationen kritisiert wurde. So warnte der Deutsche Anwaltsverein (DAV) vor dem „Tabubruch", Ermittlern neue Befugnisse zur DNA-Analyse zu geben. DAV-Hauptgeschäftsführer Philipp Wendt sprach von einem „unzulässigen Eingriff in das Persönlichkeitsrecht", wenn künftig DNA-Spuren unbekannter Personen vom Tatort auf die Farbe von Augen, Haut und Haaren analysiert werden dürfen. Auch das ungefähre Alter von Gesuchten soll ermittelt werden können, um Fahndungen zu erleichtern. Wendt forderte, der Bundestag solle den Passus kippen. Der Kriminologe Christian Pfeiffer kritisierte, der Entwurf wecke „Erwartungen, die nicht erfüllbar sind". Die Wissenschaft sei noch nicht weit genug. Vorhersagen liegen bei blonden Haaren z. B. in nur 70% der Fälle richtig: „Der Innenminister muss Geld investieren, damit die Forschung vorankommt." Im Bundesrat wurden schon Änderungswünsche vorgetragen. Die niedersächsische Justizministerin Barbara Havliza (CDU) will erreichen, dass auch das Alter von Beschuldigten ermittelt werden darf, wenn dieses nicht aus Dokumenten sicher hervorgeht: „Eine DNA-Untersuchung ist für den Betroffenen ein wesentlich geringerer Eingriff als die bisherigen Methoden. Es ist ein Unterschied, ob ein Röntgengerät zum Einsatz kommt oder ein Wattestäbchen." DNA lässt sich mit einer Speichelprobe gewinnen. Sollte das neue Gesetz verabschiedet werden, so müssten die Behörden bundesweit knapp 5 Mio. € allein für neue Analysegeräte ausgeben (Streit um DNA-Analysen zu Fahndungszwecken, Der Spiegel Nr. 44 26.10.2019, 26).

Bund

Daten-Ethikkommission legt Bericht vor

Die Daten-Ethikkommission der Bundesregierung, ein Gremium aus JuristInnen, WirtschaftsvertreterInnen und VerbraucherschützerInnen, das 2018 von der damaligen Bundesjustizministerin Katarina Barley (SPD) und Bundesinnenminister Horst Seehofer (CSU) ins Leben gerufen wurde, um ethische Leitlinien für die Digitalisierung zu erarbeiten, legte am 23.10.2019 ihren Bericht vor. Es geht um Rahmenbedingungen zur Anwendung künstlicher Intelligenz und die Stärkung der Rechtssicherheit für die VerbraucherInnen bei gleichzeitiger Offenheit für die Chancen der Digitalisierung. Der Tenor des Gutachtens ist: Ohne staatliche Kontrolle im Netz nehmen Grundrechte Schaden.

Die Medizinethikerin Christiane Woopen, eine der SprecherInnen der Daten-Ethikkommission, erklärte: „Die große Herausforderung besteht darin, die Vorteile der Digitalisierung im Alltag und in der Wirtschaft voran zu bringen. Dabei muss aber auch Rechtssicherheit bestehen." Bei allen Chancen brächten digitale Technologien auch „erhebliche Risiken für die Grundrechte von Menschen". In dem Gutachten warnt die Kommission vor ethisch nicht vertretbaren Datennutzungen wie „Totalüberwachung, die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten" oder „dem Demokratieprinzip zuwiderlaufender Beeinflussung politischer Wahlen". Die „systematische Schädigung von Verbrauchern" müsse bekämpft werden. Vorhandene Gesetze würden „bislang nicht in ausreichender Weise genutzt – insbesondere gegenüber marktmächtigen Unternehmen".

Die Kommission lehnt die Anerkennung von „Dateneigentum" ab, also die unwiderrufliche Übergabe personenbezogener Daten wie z. B. Gesundheitsinformationen an Versicherungskonzerne. Die Verwendung der Daten zur personalisierten Risikoeinschätzung sollten eng begrenzt werden. Zudem fordert das Gutachten, dem „erheblichen Vollzugsdefizit" beim Schutz von Kindern und Jugendlichen im digitalen Raum abzuhelfen. Für algorithmische Systeme sollen künftig mehr Kontrolle und eine gestaffelte Risikoeinschätzung gelten. Die Kommission empfiehlt, sie in fünf Risikoklassen einzuteilen, je nach drohendem Schaden für Verbraucherrechte. Algorithmen mit „unvertretbarem Schädigungspotenzial" sollen verboten werden können. Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands, erläutert „Wir brauchen Aufsichtsinstitutionen, die Algorithmen überprüfen und sicherstellen, dass Verbraucher nicht benachteiligt werden." Fragt man ihn, wie so viel Netzkontrolle funktionieren soll, verweist er auf die Frankfurter Börse. Dort sei Algorithmenkontrolle längst etabliert: „Wo ein Wille war, war auch ein Weg" (von Bullion, Aufsicht für Algorithmen, SZ 23.10.2019, 18; Link zum Gutachten: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html).

Bund

GFF erhebt Verfassungsbeschwerde gegen BKA-G

Ein Jahr nachdem das Bundeskriminalamt (BKA) in einem BKA-Gesetz (BKA-G) neue Befugnisse zum Speichern von personenbezogenen Daten

erhalten hat, werden diese Regeln durch das Bundesverfassungsgericht (BVerfG) überprüft. Die Organisation Gesellschaft für Freiheitsrechte (GFF) bemängelt in einer Verfassungsbeschwerde, dass „weite Kreise der Bevölkerung" in Gefahr geraten, durch einen Eintrag in der neuen BKA-Datenbank „stigmatisiert" zu werden. Die neu eingeführten Löschfristen seien „teils inkonsistent" und „in hohem Maße unbestimmt", so der Vorsitzende der GFF, der Berliner Richter Ulf Buermeyer.

Eine Sprecherin des BVerfGs bestätigte, dass die Klageschrift bereits im Mai 2019 eingereicht wurde. Der Erste Senat hatte das Gesetz schon einmal geprüft und die umfangreichen Befugnisse der Ermittler zur Terrorabwehr 2016 zum Teil für verfassungswidrig erklärt. Damals stellten die Richter „in etlichen Einzelvorschriften unverhältnismäßige Eingriffe" fest. Das Gesetz musste daraufhin überarbeitet werden; die neue Fassung ist seit Mai 2018 in Kraft. Der GFF geht das nicht weit genug. Sie mahnt eine „noch nicht ausgeleuchtete Lücke im Verfassungsrecht" an. Kontaktpersonen von Verdächtigen könnten zu leicht selbst Opfer heimlicher Überwachung werden. Die GFF hält weiterhin den Einsatz von Trojanern zum Ausspähen von Computern und Handys für verfassungswidrig.

Das BKA darf in seiner Datenbank nicht nur Verurteilte, Beschuldigte und Verdächtige speichern, sondern auch Personen, die bisher keine Straftat verübt haben, bei denen aber trotzdem ein „Anlass" bestehe, „weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden". Eine vergleichbare Regelung gab es schon früher. Die GFF bemängelt aber, bei der BKA-G-Reform sei es versäumt worden, die Prognosekriterien genauer zu fassen. Verfassungsrechtlich überprüft worden ist diese Präventiv-Speicherung bisher noch nie.

Auch darf das BKA vormals Verdächtige einer Straftat selbst dann weiterspeichern, wenn sie vor Gericht freigesprochen wurden oder ihr Strafverfahren eingestellt worden ist. Das BKA-G verpflichtet das BKA nur dann zur Löschung, wenn das Gericht dem Betroffenen ausdrücklich bescheinigt hat, dass seine Unschuld erwiesen ist. So etwas komme in der Praxis selten vor, kritisiert der Mainzer Rechtsprofessor Matthias Bäcker. Bäcker hat die GFF-Verfassungsbeschwerde formuliert und vertritt den Fall in Karlsruhe: „Der Beschuldigte hat auch keine prozessuale Möglichkeit, eine solche Feststellung zu erwirken." Daher soll auch diese Regelung – die es in ähnlicher Form ebenso schon früher gab – erstmals verfassungsrechtlich überprüft werden.

Ein Kernpunkt der 2018 reformierten Datenverarbeitung des BKA war es, die bisherige Trennung zwischen den Daten vieler Betroffener aufzuheben. Wo bisher einzelne Dateien wie „Gewalttäter Sport" oder „Politisch motivierte Kriminalität – rechts" nebeneinander existierten, wurden diese Dateien zu einem großen Datenpool zusammengelegt. Das Ziel dieser Reform war es zu vermeiden, dass die BKA-ErmittlerInnen langwierig in einzelnen Dateien suchen müssen. Sie sollen mit geringerem Aufwand das gesamte Wissen digital zur Verfügung haben, u. a. um leichter Zusammenhänge erkennen können, zum Beispiel Querbezüge zwischen Terrorismus und organisierter Kriminalität. Gemäß der Verfassungsbeschwerde der GFF trennt das BKA dabei aber nicht mehr sauber genug zwischen Personen, die einst wegen bloßer Bagatelldelikte oder sogar nur als Zeugen in eine BKA-Datei hineingelangt sind, und Schwerkriminellen. Damit würde das Zweckbindungsprinzip ausgehebelt. Wenn die Polizei eine BürgerIn nur zu einem bestimmten Zweck, zum Beispiel der Aufklärung eines Fahrzeugdiebstahls, speichern durfte, dann dürfen die Daten traditionell auch nur zu diesem Zweck genutzt werden. Diese rechtsstaatliche Sicherung gehe verloren, so die Kritik, wenn alle Daten in einem großen Pool landen.

Zwar sieht das BKA-G vor, dass besonders heikle persönliche Daten weiterhin nur zu besonders wichtigen Zwecken genutzt werden dürfen. Die BKA-Ermittler sollen „abgestufte" Zugriffsrechte auf die Daten erhalten. Sobald jedoch ein besonders wichtiges Ziel wie die Terrorabwehr im Raum steht, kann das BKA, so die GFF, recht mühelos Daten auch von Kleinkriminellen oder von gänzlich Unverdächtigen heranziehen und lange in seiner Datenbank behalten. Im Namen der Terrorabwehr könne das BKA „neben Daten über ´Gefährder` auch etwa Daten über Dritte ohne besonderen Anlass bevorraten, wenn sich nur irgendwie begründen lässt, dass diese Daten einmal zur Terrorabwehr" beitragen können, heißt es in der Beschwerdeschrift. Schon „lose und oberflächliche soziale Kontakte" könnten genügen. Dies könne für Betroffene spürbare Folgen haben, „wenn eine Polizeibehörde in einer tatsächlichen oder vermeintlichen Krisensituation zur Lagebeurteilung auf die bevorrateten Daten zugreift".

Die Verfassungsbeschwerde ist im Namen von fünf BürgerInnen erhoben worden, die fürchten, unter den neuen Regeln zu leiden. Zu ihnen gehört die Strafverteidigerin Ricarda Lang aus München, die häufig Terrorverdächtige vertritt und deshalb viel mit deren Umfeld kommuniziert. Neben einer weiteren Strafverteidigerin beteiligen sich auch zwei Fanaktivisten der Fußballvereine 1860 München und Werder Bremen, die sich schon bisher gegen ihre Speicherung in einer „Informationsdatei Fußball" beziehungsweise einer Datei „Gewalttäter Sport" gewehrt hatten. Hinzu kommt der Münchner linke Aktivist Kerem Schamberger, der seit längerem beklagt, bei Grenzkontrollen stets aufgehalten zu werden, weil er als „potenzieller" künftiger Straftäter in Polizeidatenbanken gespeichert sei (Steinke, Verfassungsbeschwerde gegen BKA-Gesetz; SZ 04.09.2019, 1, 5; Deck, Verfassungsbeschwerde gegen nachgebessertes BKA-Gesetz, www.spiegel.de 04.09.2019).

Bund

Upskirting soll strafbar werden

Gemäß dem Willen von Bundesjustizministerin Christine Lambrecht (SPD) soll das heimliche Fotografieren unter Röcke und Kleider durch eine Änderung des Strafgesetzbuchs unter Strafe gestellt werden: „Wer Frauen und Mädchen heimlich unter den Rock fotografiert, greift massiv in ihre Intimsphäre

und ihr Persönlichkeitsrecht ein." Sogenanntes Upskirting weiterhin höchstens als Ordnungswidrigkeit zu ahnden, biete keinen effektiven Schutz und mache Tätern nicht klar, dass ihr „demütigendes und herabwürdigendes Verhalten" absolut inakzeptabel sei. „Aktuell erarbeiten wir Vorschläge, wie eine solche Strafnorm aussehen kann, und wollen das zügig umsetzen." Mitte August 2019 hatte Rheinland-Pfalz eine entsprechende Initiative im Bundesrat in Aussicht gestellt. Zuvor hatten Baden-Württemberg, Bayern und Nordrhein-Westfalen mitgeteilt, einen Gesetzentwurf im Bundesrat einzubringen. Darin ist vorgesehen, dass die Tathandlung mit bis zu zwei Jahren Gefängnis sanktioniert werden kann. Bestraft werden soll auch, wer solche Aufnahmen im Internet teilt oder per Messenger verschickt. Auch Schleswig-Holstein wollte sich daran beteiligen.

Bislang sind solche Aufnahmen in der Regel nicht strafbar – es sei denn, das Opfer hält sich in einer Wohnung auf und die Aufnahmen verletzen den höchstpersönlichen Lebensbereich. Zwei junge Frauen hatten eine Onlinepetition gestartet, um Upskirting unter Strafe zu stellen. Bis Mitte September 2019 hatten sich schon mehr als 85.000 Unterzeichnende ihrer Initiative angeschlossen (Heimliches Fotografieren unter Röcke soll bestraft werden, www.zeit.de 12.09.2019; Strafen für „Upskirting", SZ 13.09.2019, 7).

Bund

BSI warnt vor BSI-Fake-Mails

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte Ende Juli 2017 vor einer Spam-Mail, die angeblich von ihm stammt: „Getarnt als BSI verschicken Kriminelle aktuell Schadsoftware per Mail." Die mit Bundesadler im Briefkopf versehenen Mails stammten nicht vom BSI, auch wenn als Absenderadresse „meldung@bsi-bund.org" genannt ist. Im Fließtext warnt die Behörde den Adressaten angeblich vor einem „möglichen Missbrauch Ihrer Daten". Angehängt hat der Absender einen „Datensatz" mit weiteren Informationen. Das BSI, gegründet 1991, mit Sitz in Bonn ist als nationale Behörde für Cybersicherheit dem Bundesinnenministerium unterstellt. Adressaten sollten Mails, Links und Anhänge dieses Absenders also nicht öffnen. Immer wieder schicken Kriminelle Mails mit schädlichen Anhängen an Privatleute und Unternehmen. Nutzer sollten daher grundsätzlich prüfen, ob sie den Adressaten der Mail kennen, rät das BSI, und ob Betreffzeile und Fließtext Sinn ergeben. „Ein unpräzise formulierter E-Mail-Betreff wie ´Ihre Rechnung` oder ´Mahnung` deutet auf eine Spam-Mail hin", warnt die Behörde. Auch sollten sich Adressaten fragen, ob sie überhaupt einen Anhang von diesem Absender – beispielsweise die Rechnung für eine Bestellung im Onlineshop – erwarten (Behörde warnt vor Spam – angeblich von ihr selbst, SZ 26.07.2019, 19).

Bund

KfZ-Sachverständige fordern Datenzugang

Der zunehmende Einsatz moderner Fahrerassistenzsysteme und die Entwicklung hin zum automatisierten und vernetzten Fahren bedeutet für die KÜS (Kfz-Überwachungsorganisation freiberuflicher Kfz-Sachverständiger), dass sie für die gesetzlich vorgeschriebenen Fahrzeugprüfungen Zugang zu den relevanten Daten haben müssen, um ihre Aufgabe im Sinne der Verkehrssicherheit für alle zu erfüllen. Beim Einbau der ersten elektronischen Systeme in neuen Fahrzeugen in den 1980er und 1990er Jahren konnten nur die jeweiligen Hersteller Daten dieser Systeme pflegen und auslesen. Mit der Verschärfung der Abgasgrenzwerte wurden die Schnittstelle und die Datenformate normiert, so dass über die gesetzlich vorgeschriebene OBD (On Board Diagnostic)-Buchse relevante Werte auch bei der Abgasuntersuchung im Rahmen der HU ausgelesen werden konnten.

Meistens sind nur diese Daten für die Überwacher lesbar, andere Informationen dagegen häufig herstellerspezifisch formatiert. Für sie ist dann eine spezielle Übersetzung notwendig, an der unter anderem auch die Sachverständigenorganisation KÜS arbeitet. Aus Gründen der Cyber-Sicherheit beginnen einige Hersteller, die nicht gesetzlich geregelten Informationen zu verschlüsseln, um den Zugriff auf die Schnittstelle und die Daten gegen den Zugriff Unberechtigter zu unterbinden – die dann beispielsweise den Motor während der Fahrt stoppen könnten. Die KÜS geht davon aus, dass alle Fahrzeughersteller ihre Daten verschlüsseln werden. Sie fordert dem gegenüber einen freien, uneingeschränkten Zugang zu allen Daten, die für die gesetzlich geregelten Fahrzeugprüfungen und deren Weiterentwicklung unabdingbar sei. Dies betreffe die Überwachungsinstitutionen, das Kfz-Gewerbe und nicht zuletzt die VerkehrsteilnehmerInnen: „Die Datenhoheit muss beim Fahrzeughalter liegen." Ein Datenmonopol der Hersteller sei kontraproduktiv, da es allen mit dem Fahrzeug Befassten wichtige Daten vorenthalte. Eine Anpassung der Daten durch die Hersteller ist mittlerweile auch ohne Werkstattaufenthalt möglich. Mit dem Over-the-Air-Verfahren können Funktionen und Daten geändert werden, ohne dass der Halter oder andere davon etwas erfahren. Daher fordert die KÜS auch eine unabhängige Dokumentation und Überprüfung der aktuellen Softwareversionen und von Updatevorgängen.

KÜS-Geschäftsführer Peter Schuler erklärte: „Wir sehen bei den sehr schnell voranschreitenden Technologien im Bereich des automatisierten Fahrens Handlungsbedarf. Die Überprüfung der Fahrzeuge durch die Prüforganisationen muss möglich sein." Ein Lösungsansatz für den Zugang zu Fahrzeugdaten ist aus Sicht der KÜS ein sogenanntes Trust-Center, in dem die Speicherung und Verwaltung über eine neutrale, von den Herstellern unabhängige Fahrzeugdatenplattform erfolgen. Diese soll von einer beliehenen, also hoheitlichen Stelle betrieben werden. Gefordert wird zudem eine Zertifizierung des gesamten Weitergabeprozesses von Fahrzeugdaten, um sicherzustellen, dass ausschließlich Befugte Zugang zu den Daten der herstellerunabhängigen Fahrzeugdatenplattform

bekommen. Ziel ist eine Standardisierung sowie die Verankerung in den internationalen Typgenehmigungsvorschriften von Fahrzeugen (John, KÜS fordert Zugang zu den Daten, www.automobilwoche.de 10.09.2019).

Bund

Arbeitsunfähigkeitsbescheinigung soll digital werden

Die Bundesregierung hat Ende September 2019 beschlossen, die Krankmeldung auf Papier, den so genannten „gelben Schein“, abzuschaffen. Die Arbeitgeber sollen künftig elektronisch über Beginn und Dauer der Arbeitsunfähigkeit eines erkrankten Arbeitnehmers informiert werden. Die Regelungen sind Teil des „Bürokratieentlastungsgesetz III“, das vom Bundestag und vom Bundesrat verabschiedet werden muss und zum 1.1.2021 in Kraft treten soll.

Rund 77 Millionen Arbeitsunfähigkeitsbescheinigungen wurden im Jahr 2017 ausgestellt. Mit der digitalen Krankschreibung, die in § 109 SGB IV geregelt wird, will man den Aufwand verringern: Die Krankenkasse, die ohnehin die Daten erhält, soll eine elektronische Meldung erstellen, die der Arbeitgeber abrufen kann. Der Versicherte selbst soll vom Arzt weiterhin eine Papierbescheinigung als Beweismittel erhalten. Von der Änderung nicht erfasst werden geringfügig in Privathaushalten Beschäftigte. Durch Verschlüsselung der Daten beim Austausch und Authentisierungsverfahren soll die Vertraulichkeit der Kommunikation gewährleistet bleiben. Nach einem halben Jahr ist eine Evaluierung der Neuregelung geplant.

Gemäß der Gesetzesbegründung sollen durch die digitale Krankschreibung auch die im Alltag immer wieder auftretenden Konflikte darüber vermieden werden, ob der gelbe Zettel pünktlich vorlag oder nicht. Für die Krankenkassen wird durch die Gesetzesänderung ein Mehraufwand von insgesamt 150 Mio. Euro vorausgesagt; für die Wirtschaft soll sich dagegen der Bürokratieaufwand um 549 Millionen Euro verringern. Insgesamt sollen Unternehmen durch das „Bürokratieentlastungsgesetz III“ über verschiedene Maßnahmen pro Jahr mindestens 1,1 Milliarden Euro einsparen können. Neben der digitalen Krankschreibung soll es künftig auch bei elektronisch gespeicherten Steuerunterlagen Erleichterungen geben. Zudem ist bei Hotelübernachtungen ein digitaler Meldeschein vorgesehen (TW).

Bundesweit

R+V-Versicherung liest beim Bankkonto mit

Die Wiesbadener R+V-Versicherung testet ein Angebot, bei dem das Konto einer Raiffeisen- oder Volksbank elektronisch ausgewertet wird: Wer für eine bestimmte Summe einkauft, erhält automatisch ein Angebot zur Absicherung der gekauften Gegenstände, etwa eines Fernsehers, eines neuen Laptops oder eines Fahrrads. Damit sollen junge Kunden angelockt werden: „Glückwunsch! Viel Spaß mit Deinem Einkauf über 750 Euro.“ So meldet sich eine App der R+V-Versicherung, wenn die KundIn sich vorher dort angemeldet hat. Das Gerät sei kostenlos für fünf Tage gegen Beschädigung versichert, „sogar dann, wenn Du selbst daran schuld bist“. Nach fünf Tagen kann die stolze BesitzerIn ihre Erwerbung dann gegen eine Prämie weiter versichern. Andere einzelne Wertgegenstände kann sie per Foto zu der Sammlung in der App hinzufügen und so absichern. Der Test von R+V wird mit KundInnen der Volksbank Berlin durchgeführt. Die App erfährt über die Kundenkäufe durch eine permanente Kontoanalyse. Diese wird durch die EU-Zahlungsdirektive von 2018 (PSD 2) ermöglicht, wenn die KundIn einwilligt. Anja Hartwig, die Projektverantwortliche bei der R+V erläutert: „Das System weiß, wenn mit Bankkarte oder Kreditkarte ein wertvoller Gegenstand erworben wurde“. Das muss nicht nur für Konten bei den genossenschaftlichen Raiffeisen- und Volksbanken gelten: „Die Kundin oder der Kunde können Konten bei anderen Banken problemlos in die App integrieren.“

Viele Versicherer haben das Problem, dass sie die internet-affine junge Generation nicht erreichen. Die traditionellen Vertriebswege über Vertreter oder Bankschalter versagen hier zunehmend. Wenn sich junge Menschen für den Abschluss interessieren, tun sie das meistens im Internet bei Vergleichsportalen oder Direktanbietern. Traditionelle Versicherer müssen fürchten, diese Zielgruppe für immer zu verlieren, auch wenn sie älter wird. Das Projekt von R+V soll dazu beitragen, mit dem Problem fertigzuwerden. Die Gesellschaft gehört den genossenschaftlichen Raiffeisen- und Volksbanken und kooperiert eng mit ihnen. Das neue Angebot kombiniert zwei Digitalisierungstrends, über die in der Finanzbranche viel geredet wird: die Versicherung für einzelne Gegenstände, bei der die Police auch gleichzeitig eine Liste der Besitztümer ist, und die nun zulässige Technik der permanenten Kontenanalyse. Wenn die KundIn die „Insurebox“-App nutzt und zugestimmt hat, „interessante Angebote“ ihrer Bank und ihres Versicherers erhalten zu wollen, gewährt sie dafür den Zugriff auf ihre Konten und Kreditkarten. Dann liest der Roboter des Versicherers ständig mit.

Der Hauptunterschied zur klassischen Hausratpolice ist der eingebaute Schutz gegen selbst verschuldete Schäden. Das Angebot ist nicht billig. Hartwig: „Für Gegenstände mit einem Wert von 250 Euro bis 1.000 Euro kostet der Schutz 45 Euro bis 79 Euro pro Jahr.“ Mit der Versicherung einzelner Gegenstände statt der traditionellen Hausratversicherung versuchen schon andere Versicherer und Start-ups zu punkten. Die Ergebnisse sind verschieden. Die Schweizer Gesellschaft Baloise ist begeistert von ihrer Gegenstandsversicherung. Auch die Start-ups One in Deutschland und Trov in den USA bieten solche Policen an. Eine Reihe von Versicherern, darunter Munich Re und Axa, unterstützen die neuen Anbieter. Allerdings hat Trov seine Gegenstandsversicherung in Großbritannien zum 01.10.2019 geschlossen. Die Kombination der Gegenstandsversicherung mit der Bankkontoauswertung gilt bei vielen Versicherern als Königsweg, um im digitalen Zeitalter wieder mit den KundInnen in Kontakt zu kommen. KundInnen nutzen normale Versicherungs-Apps kaum, es sei

denn, sie reichen in der privaten Krankenversicherung Arztrechnungen und Rezepte online ein. Dagegen nutzen sie ihre Bank-App mehrmals in der Woche, manchmal sogar mehrmals pro Tag (Fromme, Wenn der Roboter das Konto liest, SZ 06.08.2019, 18).

Bundesweit

Kfz-Versicherungsrabatt mit Dashcam

Die Versicherungsgruppe Die Bayerische bietet AutofahrerInnen einen Rabatt von 15% bei ihrer Kfz-Versicherung, wenn sie eine Dashcam ins Auto einbauen. Das gilt für die Haftpflicht sowie für eine etwaige Teil- oder Vollkaskoversicherung. Angebracht wird die Kamera entweder an der Windschutzscheibe innen oder auf dem Armaturenbrett, um den vorausfahrenden Verkehr aufzeichnen zu können.

Die erforderliche Kamera von Nextbase kann mit einem 5%- Nachlass bei den Elektronikmärkten Saturn oder Mediamarkt oder bei Autoteile Unger (ATU) erworben werden. Die KundIn kann unter mehreren Kameras des Herstellers mit Preisen zwischen rund 70 und 216 € wählen, die sich durch ihre Auflösung, ihre Bildschirme und Konnektivität voneinander unterscheiden. Der BGH hatte am 15.05.2018 entschieden, dass die Nutzung von Dashcam-Aufnahmen zur Klärung von Haftungsfragen bei Unfällen nicht grundsätzlich ausgeschlossen ist, sprach sich aber gegen eine permanente Aufzeichnung des Verkehrsgeschehens durch Autofahrer aus (DANA 2/2018, 119 f.). Die Kameras müssen deshalb im sogenannten Loop-Recording-Verfahren arbeiten, wobei alte Aufnahmen kontinuierlich überschrieben und nur bei Unfällen dauerhaft gesichert werden, wofür Bewegungssensoren sorgen.

Die Versicherung führt an, dass eine Dashcam zu einem sichereren Fahrverhalten führen kann, weil die Kamera auch das eigene Fahrverhalten aufzeichnet. Ein entscheidendes Argument für die Verwendung einer Dashcam sei zudem die schnelle Klärung von Unfallhergängen. Sie unterstütze bei der Klärung der Schuldfrage, könne Betrugsversuche vermeiden und soll Zeit und Kosten langwieriger Verfahren sparen (Donath, Kfz-Versicherungsrabatt bei Dashcam-Nutzung, www.golem.de 01.10.2019).

Bundesweit

E-Mail-Betrugsversuch nach Thomas-Cook-Pleite

Der insolvente Reisekonzern Thomas Cook warnte seine KundInnen in Deutschland vor einer E-Mail-Betrugsmasche. Diese wurden dazu aufgefordert, sensible Daten wie beispielsweise Pass- oder Kreditkartendaten preiszugeben. Die verschickten E-Mails sähen aus wie offizielle Nachrichten des Reiseunternehmens und stellen den EmpfängerInnen eine Erstattung ihrer Thomas Cook-Reise in Aussicht. Das Unternehmen stellte dazu klar: „Thomas Cook hat zu keiner Zeit Mails dieser Art an Kunden verschickt. Bitte ignorieren Sie diese Mails und löschen diese.“ KundInnen der Thomas Cook Veranstalter (Thomas Cook Signature, Thomas Cook Signature Finest Selection, Neckermann Reisen, Öger Tours, Bucher Reisen und Air Marin), die bis einschließlich 31.10.2019 verreisen wollten, konnten ihre Reise wegen der Insolvenz nicht antreten. Erstattungs-Ansprüche müssen an den Insolvenzverwalter gerichtet werden. Nach der Insolvenz des britischen Mutterkonzerns hatte auch die deutsche Thomas Cook am 25.09.2019 einen Insolvenzantrag gestellt (Thomas Cook warnt Kunden vor E-Mail-Betrug, www.sueddeutsche.de 29.09.2019).

Bundesweit

Deutschen geht Datenschutzbewusstsein ab

Gemäß einer aktuellen Umfrage mit 3.200 Teilnehmenden zur Risikokompetenz ist Datenschutz den Deutschen kaum einen Cent wert. In Anbetracht aktueller Großthemen wie Digitalisierung, Klimawandel, Alter, Geld oder Gesundheit attestiert der Risiko-Report 2019 der Ergo-Versicherung den BundesbürgerInnen, die Sorge um die eigene Sicherheit gerne abzugeben. Besonders in Bereichen der Digitalisierung scheuen die meisten Befragten noch vor dem Neuen und halten am Altvertrauten fest. Neun von zehn Personen schenken ihrem Arzt mehr Glauben als einer Diagnose, die auf Künstlicher Intelligenz basiert. Auch bei der Pflege ziehen 85% der Befragten einen realen Menschen einem Pflegeroboter vor. Gleiches gilt für die Finanzberatung: Hier vertrauen 69% eher einem Finanzberater als einem virtuellen Assistenten.

Ein recht sorgloses Bild ergeben die Daten zum Bereich der Sozialen Medien. Obwohl bekannt ist, dass Facebook, Whatsapp oder Instagram Daten ihrer Nutzenden sammeln und verkaufen, sind 75% der Deutschen nicht gewillt, für den Schutz ihrer Daten überhaupt Geld auszugeben, auch nicht für Online-Angebote, wenn gegen Gebühr die Privatsphäre geschützt würde. Mark Klein, Vorstandsvorsitzender Ergo Digital Ventures meinte: „Eine gute Aufklärung an Schulen zum Thema Datenschutz fehlt in Deutschland häufig.“ Immerhin 40% der Deutschen gaben unter den meist gefürchteten Risiken nicht länger die Angst vor Terrorismus oder Krieg an, sondern jene vor Unwettern und Naturkatastrophen als Folge des Klimawandels (Deutsche übernehmen immer weniger Eigenverantwortung, www.springerprofessional.de 04.10.2019).

Baden-Württemberg

CDU will Polizeirecht weiter verschärfen

Ein buntes Bündnis von Linken, Fußballfans und Jugendgruppen rief am 12.10.2019 zu einer landesweiten Demonstration auf gegen die von CDU-Innenminister Thomas Strobl beabsichtigte Verschärfung des Polizeigesetzes. Hintergrund war ein nicht veröffentlichter 160-seitiger Entwurf, mit dem Strobl Terroranschläge verhindern und in rechtlich geschützte Räume wie heimische PCs eindringen möchte. Dass er dies will, hatte er schon 2018 verkündet. Der Inhalt des geplanten Gesetzespakets ist im Wesentlichen bekannt. Es geht um zusätzliche Befugnisse für die Polizei: von der Online-Durchsuchung über

die Schleierfahndung (verdachtsunabhängige Kontrollen) bis hin zum Recht für die Polizei, BodyCams auch in Wohnungen zu benutzen. Bekannt ist auch, dass sich die mitregierenden Grünen gegen die Pläne sperren. Fraktionschef Andreas Schwarz erklärt ein ums andere Mal, man habe vom „Rückgaberecht Gebrauch gemacht".

Doch hinter den Kulissen ist Bewegung. Innen-Staatssekretär Wilfried Klenk (CDU), der das Thema seit Sommer 2019 bearbeitet, und der Grünen-Innenexperte Uli Sckerl haben sich mehrfach getroffen. Sckerl berichtete darüber am 08.10.2019 seiner Fraktion. Auch die Grünen-Landesvorsitzenden reden mit und dies nicht immer mit dem selben Zungenschlag wie Sckerl. So ist es schwierig zu beurteilen, inwiefern „die Grünen" bereit sind, die Grenze zwischen Sicherheit und Bürgerrechten zu verschieben.

Die Fraktion zeigt sich jedenfalls eher bereit als die Parteispitze, der Polizei den Einsatz von BodyCams in geschlossenen Räumen zu gestatten; nicht in Wohnungen, wie Strobl dies will, aber doch in Clubs oder Gaststätten. Sicherheitspolitiker wie der CDU-Abgeordnete Siegfried Lorek halten das zwar für unzureichend und argumentieren, fast täglich würden Beamte zu häuslichen Streitereien gerufen. Die CDU bohrt weiter und schlägt vor, den Kameraeinsatz auf Fälle mit Gefahr im Verzug zu beschränken.

Da Strobl Maximalforderungen vorgelegt hat, verfügt er über Verhandlungsmasse. So soll er bereit sein, auf die präventive DNA-Untersuchung zu verzichten. Dabei geht es um Spurenmaterial unbekannter Herkunft, das zur Verhütung von Straftaten auch auf Geschlecht, Haar- oder Hautfarbe untersucht werden darf. Auch die Schleierfahndung würde der CDU-Mann wohl opfern, wenn die Polizei dafür das Recht erhält, bei Großveranstaltungen Personenkontrollen vorzunehmen. Außerdem will er, dass Verdächtige für eine bestimmte Zeit präventiv in Gewahrsam kommen können und stößt damit bei den Grünen nicht auf völlig taube Ohren. Die Online-Durchsuchung von PCs jedoch gilt bei den Grünen als unverhandelbar.

Bis zum Jahreswechsel 2019/2020 soll weiter verhandelt werden. Gleichzeitig treibt Strobl ein Projekt voran, das sich „Sicherer öffentlicher Raum" nennt. Es geht auf den Koalitionsvertrag zurück und hat zum Ziel, das Sicherheitsgefühl der BürgerInnen auf vielen Ebenen zu stärken. Deshalb sind in die Arbeitsgruppe gleich fünf Ministerien eingebunden. So überlegt man etwa im Verkehrsministerium, die Präsenz der Polizei in Bussen und Bahnen zu verstärken, indem man auch KripobeamtInnen kostenlos fahren lässt – bisher dürfen das nur Uniformierte. Im Justizministerium wiederum sinniert man, wie Messerangriffe schärfer geahndet werden können. Das Sozialministerium wiederum arbeitet an Konzepten, das Nachtleben in Großstädten sicherer zu machen. So soll bis zum Jahresende ein bunter Strauß von Einzelmaßnahmen entstehen (Rieger, Strobl ringt mit den Grünen um mehr Rechte für Polizei, www.stuttgarter-nachrichten.de 11.10.2019).

Bayern

Ermittlungen gegen Spionagesoftware-Hersteller Finfisher

Die Staatsanwaltschaft München I ermittelt gegen einen der bekanntesten deutschen Hersteller von auf Handys aufgespielter Spionagesoftware: die Finfisher GmbH in München. Finfisher-Software soll illegal – ohne Erlaubnis der zuständigen Behörde, des Bundesamtes für Wirtschaft und Ausfuhrkontrolle – exportiert worden sein. Eine Sprecherin der Staatsanwaltschaft teilte mit, man gehe dem Verdacht des „Verstoßes gegen bestimmte Ausfuhrbestimmungen" nach. Ermittelt werde gegen „die verantwortlichen Geschäftsführer und Mitarbeiter der Finfisher GmbH und zweier weiterer GmbHs". Auslöser waren Medienberichte aus dem Jahr 2018 und eine Anzeige durch die Organisationen Reporter ohne Grenzen (RoG), Netzpolitik.org, Gesellschaft für Freiheitsrechte (GFF) und European Center for Constitutional and Human Rights (ECCHR), die sich gegen Überwachung engagieren. Das Unternehmen wollte sich auf Nachfrage zu dem Vorgang nicht äußern.

Spähsoftware wird rechtlich zwar nicht als Waffe eingestuft, wird aber als so heikel bewertet, dass ihr Export nur unter bestimmten Bedingungen erlaubt ist. Seit 2015 werden Software und Geräte, mit denen sich Menschen ausspionieren lassen, als sogenannte Dual-Use-Produkte klassifiziert, die zivilen wie militärischen Zwecken dienen können. Ähnliche Regeln gelten etwa für Chemikalien, die sowohl für Gift als auch für Antriebstechnik benutzt werden könnten. Um Missbrauch zu vermeiden, müssen die Güter einer nationalen Behörde vorgelegt werden, bevor sie in ein Nicht-EU-Land verkauft werden. Laut der Anzeige wurde die Finfisher-Software „Finspy" in der Türkei gegen die größte Oppositionspartei CHP eingesetzt. Offenbar wurde versucht, Oppositionelle im Umfeld des „Marsches der Gerechtigkeit" auszuspähen, wie 2018 bekannt wurde. Der Marsch von Ankara nach Istanbul ein Jahr zuvor war eine Protestaktion der CHP gegen Präsident Erdoğan.

Über soziale Netzwerke wurde damals eine Webseite beworben, die vermeintlich von Sympathisierenden des Marsches betrieben wurde. Die Verbreiter nutzten den Hashtag, den die DemonstrantInnen und ihre UnterstützerInnen verwendeten. Tatsächlich befand sich auf der Webseite Schadsoftware zum Download. Die Anzeigesteller beschreiben diese so: „Nach dem Herunterladen auf ein mobiles Gerät ermöglichte diese Android-Anwendung, bei der es sich um Malware handelt, dem Angreifer den Zugang zu Telefon-und VoIP-Gesprächen, Datensystemen, Screenshots und anderen Fotos, GPS-Daten, Mikrofonen und Verbindungsdaten sowie zu verschiedenen Anwendungen, unter anderem Whatsapp, Line, Viber, Telegram, Skype, Facebook Messenger." Nach erfolgreicher Infektion hätten die digitalen Angreifer das Handy praktisch komplett überwachen können. Es habe sich dabei „mit an Sicherheit grenzender Wahrscheinlichkeit" um Finspy gehandelt.

Eine Quellcodeanalyse der Organisation Access Now, die der Anzeige zugrunde liegt, legt nahe, dass die eingesetzte Software aus dem Jahr 2016 stammt. Die Spähsoftware verwende digitale Werkzeuge, die es erst seit 2016 gibt. Sie enthalte zudem digitale Signaturen, die erst nach 2015 ausgestellt wurden. Thorsten Holz, Professor für IT-Sicher-

heit an der Ruhr-Universität Bochum, bestätigt die Analyse. Ein Sprecher des Bundeswirtschaftsministeriums gibt allerdings an, von solchen Exporten nichts zu wissen. „Die Bundesregierung hat keine solchen Einzelgenehmigungen für die Ausfuhr von Intrusion-Software erteilt." Den Anzeigestellenden zufolge muss der Export also illegal zwischen Oktober 2016 und Juli 2017 stattgefunden haben.

Finfisher verspricht auf seiner Firmenseite, „ausschließlich mit Strafverfolgungsbehörden und Geheimdiensten" zusammenzuarbeiten, um „Terror und Gewaltverbrechen zu verhindern und aufzuklären". Die Software ist aber auch berüchtigt, weil sie von undemokratischen Systemen eingesetzt wurde. Fachleuten zufolge haben sie Dutzende Staaten gegen ihre BürgerInnen eingesetzt, darunter Bahrain und Äthiopien. In Deutschland soll das Unternehmen die Bundestrojanersoftware entwickeln. Mit der soll das Bundeskriminalamt – wenn ein Richter es erlaubt – die Handys Verdächtiger überwachen (Brühl/Eckert/Tanriverdi/Wormer, Geheime Einblicke, SZ 05.09.2019, 17).

Berlin

Bußgeld gegen Delivery Hero

Die Berliner Datenschutzbeauftragte Maja Smoltczyk hat gegen die Lieferfirma Delivery Hero Bußgelder in Höhe von insgesamt 195.407 Euro wegen Verstößen gegen das Datenschutzrecht, insbesondere gegen die Datenschutz-Grundverordnung (DSGVO) verhängt. Die Firma hat vor allem Betroffenenrechte nicht beachtet und Konten von Ex-KundInnen nicht gelöscht. Der niederländische Konzern Takeway.com hat gemäß Behördenangaben als neuer Eigner des Lieferdienstes die Bescheide akzeptiert und versichert, die internen Prozesse noch einmal gründlich zu überprüfen.

Mit den Geldbußen ahndete Smoltczyk nach eigenen Angaben „diverse datenschutzrechtliche Einzelverstöße" des Unternehmens. Dieses habe in der Mehrzahl der Fälle Betroffenenrechte nicht beachtet, die sich etwa auf Auskunft über die Verarbeitung der eigenen Daten, auf Löschung oder Widerspruch beziehen. So habe Delivery Hero in zehn Fällen Konten ehemaliger KundInnen nicht gelöscht, obwohl diese jahrelang – in einem Fall sogar seit dem Jahr 2008 – nicht mehr auf der Lieferdienst-Plattform aktiv gewesen seien. Acht frühere KundInnen hatten sich ferner über unerwünschte Werbe-E-Mails beschwert. Ein Geschädigter, der der Nutzung seiner Daten für Werbezwecke ausdrücklich widersprochen hatte, erhielt dennoch weitere 15 Spamschreiben von dem Dienst, zu dem Foodora, Lieferheld und Pizza.de gehören.

Delivery Hero Germany hatte einige der Verstöße mit technischen Fehlern bzw. Mitarbeiterversehen erklärt. Aufgrund der hohen Anzahl an wiederholten Verstößen sei jedoch von „grundsätzlichen, strukturellen Organisationsproblemen" auszugehen gewesen. Trotz vielfacher Hinweise habe die Firma über einen langen Zeitraum keine ausreichenden Maßnahmen umgesetzt, „die die pflichtgemäße Erfüllung der Rechte der Betroffenen sicherstellen konnten". Die Sanktionen ergingen in zwei Bescheiden, da ein Teil der Verstöße noch nach dem alten Datenschutzrecht vor der DSGVO zu beurteilen war. Der Bundesdatenschutzbeauftragte Ulrich Kelber geht davon aus, dass es in Deutschland bald Bußgelder in Millionenhöhe geben wird (Krempl, Datenschutzverstöße: Lieferdienst Delivery Hero muss 200.000 Euro zahlen, www.heise.de 19.09.2019, Kurzlink: https://heise.de/-4533862).

Hessen

Zufallskontrollen bei POLAS-Abfragen

PolizistInnen dürfen Personenabfragen im Polizeisystem nicht für persönliche Interessen nutzen. Nach einschlägigen Vorfällen hat das Land Hessen Februar 2019 Zufallskontrollen eingeführt und musste Missbrauchsfälle feststellen. Bei jeder Kontrolle fragen die PolizistInnen ab, ob über eine betreffende Person etwas vorliegt, etwa ein Haftbefehl. So werden täglich nach Behördenangaben 40.000 bis 45.000 Personenabfragen getätigt. Darunter können auch verbotene Abfragen ohne dienstlichen Grund sein. Im Innenausschuss des Landtags erzählte Landespolizeipräsident Udo Münch jüngst von solchen Fällen: „Wir hatten einmal einen Event – Helene Fischer in Frankfurt. Da ist Helene Fischer 83 Mal in der Nacht abgefragt worden. Es ist wohl relativ unwahrscheinlich, dass Frau Fischer dort 83 Mal kontrolliert worden ist."

Deswegen hat die Polizei Zufallskontrollen eingeführt. Bei jedem 200. Abruf des polizeilichen Auskunftssystems POLAS erscheint eine Maske auf dem Bildschirm, in die der Polizist den Grund für seine Abfrage eintragen muss. Wenn die Antwort nicht plausibel ist, gehen Datenschutzbeauftragte der Polizeibehörden dem Fall auf den Grund. Diese Kontrollen wurden nach Münchs Angaben zunächst nicht immer ernst genommen: „Wir hatten am Anfang einmal den Fall, dass jemand in das Feld zum Thema Sensibilisierung ´Mickey Mouse` hineingeschrieben hat." Der betreffende Beamte sei dann „noch einmal auf die Ernsthaftigkeit der ganzen Maßnahmen hingewiesen worden". Im Jahr 2018 wurden 180 mögliche Missbrauchsfälle intern gemeldet. 2019 dürften es nach Einschätzung des Innenministeriums mehr werden, nachdem die Zufallskontrollen eingeführt worden waren: „Gemäß der bisherigen Entwicklung im laufenden Jahr kann, bei einem gleichbleibenden Verlauf bis Jahresende, von einem Anstieg ausgegangen werden." Seit Februar seien etwa 9.000 Datensätze an die Datenschutzbeauftragten überstellt worden.

Die Gefahr missbräuchlicher Abfragen war durch Fälle mit rechtsextremistischem Hintergrund öffentlich geworden. So wurden für rechtsextreme Drohschreiben, die an die Frankfurter Rechtsanwältin Seda Basay-Yildiz geschickt wurden, anscheinend Informationen über sie von einem Polizeicomputer im 1. Revier in Frankfurt abgerufen (DANA 1/2019, 38 f.). Wer dahinter steckte, konnte bisher nicht aufgeklärt werden. In einem anderen Fall hatte ein Polizist aus Dieburg Informationen aus einem Polizeisystem abgefragt und an eine Frau aus der Neonazi-Kameradschaft „Aryans" weitergegeben. Der Mann wurde wegen der Verletzung von

Dienstgeheimnissen zu einer Geldstrafe verurteilt. Das Innenministerium geht davon aus, dass er nicht aus rechtsextremer Gesinnung handelte. Oppositionsabgeordnete hatten sich verwundert geäußert über die hohe Zahl an Abfragen. Der Vorsitzende der Gewerkschaft der Polizei (GdP), Andreas Grün, nennt sie aber „ganz normal". Schließlich würden jeden Tag Kontrollen vorgenommen.

Innenminister Peter Beuth hatte nicht nur die Zufallsprotokollierung eingeführt, sondern auch einen Hinweis, der automatisch auf der POLAS-Startseite erscheint. Dort wird darauf hingewiesen, dass eine Nutzung nur zu dienstlichen Zwecken gestattet ist. Gewerkschafter Grün sagte, es gebe „Unverständnis" über diese Maßnahmen. Bei seinen KollegInnen entstehe der Eindruck, dass man wegen „ein paar schwarzen Schafen" unter Generalverdacht gestellt werde (v. Bebenburg, Polizisten missbrauchen Personenabfrage, um an Infos über Helene Fischer zu kommen, www.fr.de 03.08.2019).

Mecklenburg-Vorpommern

Widerstand gegen Entwurf eines Polizeigesetzes

Gemäß Polizeiangaben haben rund 650 Menschen am 18.08.2019 in Rostock gegen die geplante Verschärfung des Polizeigesetzes von Mecklenburg-Vorpommern protestiert und zogen unter anderem am Sitz der Kriminalpolizei vorbei. Ein Sprecher des Veranstalterbündnisses „SOGenannte Sicherheit" ging von rund 1.000 Demonstrationsteilnehmenden aus, die unter anderem von Linken, Grünen, FDP, linken Gruppen und der Fanszene von Hansa Rostock mobilisiert worden waren. Zwischenfälle gab es den Angaben zufolge nicht.

Die Gegner des Polizeigesetzes befürchten ausufernde Überwachungsbefugnisse der Polizei und beklagen mangelnde Kontrollmöglichkeiten. In Redebeiträgen wurden Überwachungsmethoden wie die Onlinedurchsuchung und die Quellen-Telekommunikationsüberwachung kritisiert. Sie sollen zukünftig schon vor dem Begehen einer Straftat eingesetzt werden dürfen, wenn ein Richter zustimmt. Die Maßnahmen sollen laut Gesetzentwurf nicht nur gegen Verdächtige, sondern auch gegen deren Umfeld eingesetzt werden dürfen. Weiter wurden fehlende Kontrollmöglichkeiten gegenüber der Polizei bemängelt. Gerade angesichts mehrerer Skandale in Mecklenburg-Vorpommern und anderen Ländern gelte: Wenn es mehr Überwachung geben solle, dann bei der Polizei durch unabhängige Kontrollstellen, hieß es in einem Redebeitrag. In Sprechchören forderten die DemonstrantInnen den Rücktritt von Innenminister Lorenz Caffier (CDU). Kritisiert wird der Entwurf der Landesregierung vom Landesdatenschutzbeauftragten, dem Deutschen Journalistenverband und Anwaltsvereinigungen. Unterstützung hierfür kam von den Polizeigewerkschaften und den Kommunalverbänden (Hunderte demonstrieren in Rostock gegen neues Polizeigesetz, www.heise.de 18.08.2019, Kurzlink: https://heise.de/-4499954).

Mecklenburg-Vorpommern

Datenschutzbehörde bremst AfD-Schulen-Prangerportal

Der Landesbeauftragte für den Datenschutz in Mecklenburg-Vorpommern, Heinz Müller, hat das Online-Meldeportal der AfD „Neutrale Schule" verboten. SchülerInnen waren dort dazu aufgerufen worden, angebliche Verstöße gegen das Neutralitätsgebot von Lehrkräften zu melden, insbesondere auch solche, die die AfD im Unterricht kritisieren. Die auf dem Portal veröffentlichten Passagen, in denen zur Meldung aufgefordert wird, müssen laut Müller bis zum 20.09.2019 entfernt werden. Andernfalls drohte er mit einem Zwangsgeld. Es dürfe nicht sein, dass LehrerInnen durch ein solches Portal in ihrer Unterrichtstätigkeit eingeschüchtert werden. Es sei selbstverständlich eine Aufgabe der Lehrkräfte, für die Demokratie, das Grundgesetz und die darin gewährleistete Menschenwürde einzutreten: „Dabei sollen sie keine Angst haben, von selbsternannten AfD-Aufpassern behelligt zu werden." Der Landesverband der AfD erhebe in dem Online-Portal nicht nur die personenbezogenen Daten der SchülerInnen, die eine Meldung verfassen. Die Partei sammele ganz gezielt auch die politischen Meinungen der gemeldeten LehrerInnen. Diese politische Meinung stehe jedoch unter besonderem rechtlichen Schutz. So stehe es in der Datenschutz-Grundverordnung. Deswegen sei ein Verbot des Portals angebracht.

AfD-Co-Landessprecher Leif-Erik Holm sprach von einer „parteipolitisch motivierten Willkürentscheidung". Der SPD-Politiker Müller habe unter Ausblendung der Fakten das geliefert, was SPD-Bildungsministerin Martin bestellt habe. „Es handelt sich sichtbar um ein abgekartetes SPD-Spielchen." Es werde versucht, einen Maulkorb zu erlassen, um mögliche Missstände an Schulen vertuschen zu können: „Dagegen werden wir juristisch vorgehen." Holm warf Landesdatenschützer Müller zudem vor, mit seiner Pressemitteilung gegen das Mäßigungsgebot verstoßen zu haben.

Bis zum ausgesprochenen Verbot war das von Anfang an umstrittene Meldeportal lediglich drei Wochen online. Bildungsministerin Bettina Martin (SPD) hatte es als „Lehrer-Pranger" bezeichnet. Es handle sich um ein ungeeignetes Instrument und gefährde den Frieden an den Schulen. SchülerInnen und Eltern würden zum Denunziantentum gegen ihre LehrerInnen aufgestachelt. Die AfD hatte das Portal nach dem Vorbild aus anderen Bundesländern wie Hamburg, Niedersachsen und Brandenburg auch für Mecklenburg-Vorpommern freigeschaltet (DANA 4/2018, 196 ff.). Innerhalb von sieben Monaten hat ein Lehrer-Meldeportal der AfD in Niedersachsen nur drei konkrete und bislang folgenlose Beschwerden erbracht. KritikerInnen halten das Angebot für eine „Luftnummer".

Der Hamburgische Datenschutzbeauftragte Johannes Caspar wies derweil die Forderung des dortigen Schulsenators Ties Rabe (SPD) zurück, ein Verbot zu prüfen. Das Portal werde in Hamburg von der AfD-Fraktion der Bürgerschaft betrieben und bei parlamentarischer Datenverarbeitung habe er weder Kompetenzen, noch gelte die DSGVO. Anwendbar sei die Datenschutzverordnung der Bürgerschaft; die Kontrolle erfolgt danach in eigener Verantwortung (Datenschützer verbietet Lehrer-Meldepor-

tal der AfD, www.ndr.de 13.09.2019; AfD-Meldeportal: Vorstoß der SPD zurückgewiesen, Kieler Nachrichten 21.09.2019, 14).

Nordrhein-Westfalen

Handballverbände verzichten auf personenbezogene Spielangaben

War es in den vergangenen Jahren noch möglich, über einen elektronischen Spielbericht unmittelbar nach Spielende die TorschützInnen und Aufstellungen der jeweiligen Mannschaften abzurufen, werden im Bereich des Westdeutschen-Handball-Verbandes (WHV) und des Handball-Verbandes Niederrhein (HVN) diese Informationen auf den offiziellen Seiten nun weggelassen. Begründet wird dies mit der angeblich bestehenden Gefahr, mit Geldstrafen aufgrund von Verstößen gegen die Datenschutz-Grundverordnung belegt zu werden. Beim Deutschen Handballbund existiert dieses Problem in den drei höchsten Ligen anscheinend nicht. Dort werden weiterhin die TorschützInnen oder gar Aktionen und Spielzüge im Internet live getickert (Keine Torschützen wegen Datenschutz, rp-online.de 16.09.2019).

Sachsen

TK-Verbindungsdaten von Anwalt ausspioniert

Auf Veranlassung sächsischer Ermittlungsbehörden wurden offenbar über Jahre hinweg die Handydaten eines Strafverteidigers erfasst. Mehrere Staatsanwaltschaften sowie das sächsische Landeskriminalamt (LKA) sammelten so Telekommunikations- (TK-) Verbindungsdaten des Dresdner Rechtsanwalts Ulf Israel. Der Anwalt geriet ins Visier der Ermittler, als er polnische Autoschieber als Mandanten vertrat. Aus einem Beschluss des Amtsgerichts Dresden geht hervor, dass dabei auch Bewegungsprofile „in Echtzeit" erstellt wurden. Weitere Akten legen den Verdacht nahe, dass es wiederholt Überwachungen zwischen 2013 und 2016 gab. Unter den abgefangenen Telefonnummern, die Israel anrief oder die ihn anwählten, sind Anschlüsse seiner Familie und die eines Kollegen, der Vorsitzender der Strafverteidigervereinigung Sachsen/Sachsen-Anhalt ist. Anwälte sollten als Berufsgeheimnisträger eigentlich weitgehend vor solchen Überwachungsmaßnahmen geschützt sein. Der Sächsische Datenschutzbeauftragte prüft den Fall. Israel hat einen Staatsanwalt wegen des Verdachts der Rechtsbeugung angezeigt. Das LKA verweist auf die Prüfung durch die Datenschutzbehörde; man könne erst danach abschließend Stellung nehmen. Die Dresdner Staatsanwaltschaft bestätigt den Eingang einer Strafanzeige, will aber nicht Stellung nehmen (Anwalt im Visier, Der Spiegel Nr. 38, 14.09.2019, 11).

Sachsen

Normenkontrolle von Grünen und Linken gegen neues Polizeirecht

Die Fraktionen der Linken und der Grünen haben eine sogenannte Normenkontrolle der im April 2019 beschlossenen Novelle des sächsischen Polizeigesetzes vor dem Verfassungsgerichtshof des Landes beantragt. Dabei geht es um eine allgemeine fachliche Prüfung, ob die beklagten Klauseln mit höherrangigem Recht vereinbar sind. Die Antragstellenden wollen mit dem Schritt erreichen, dass große Teile der neuen Befugnisse der Ermittler für nichtig erklärt werden.

Bei der Präsentation der Antragsschrift erklärte der Mannheimer Staatsrechtler Matthias Bäcker, mehrere Komplexe seien verfassungsrechtlich besonders problematisch. So habe der Gesetzgeber die Hürden für die Überwachung von Einzelpersonen etwa per Telekommunikationsüberwachung, Observation oder den Einsatz verdeckter Ermittler deutlich gesenkt. Die Polizei könnte künftig mit Blick auf „gefährliche" Personen entscheiden, welche Mittel eingesetzt werden. Es genüge, dass die Polizei anhand vager Kriterien prognostiziere, eine Person könnte einmal eine Straftat begehen. Das überarbeitete Polizeirecht definiere „Straftaten von erheblicher Bedeutung" bis hinein in den Bagatellbereich. Bei staatsschutzrelevanter Motivation seien sogar Beleidigungen oder Sachbeschädigungen erfasst. Der deutlich ausgeweitete Instrumentenkoffer dürfe auch bereits bei Vorbereitungshandlungen eingesetzt werden, also etwa gegen eine Person, die „möglicherweise Heizöl kaufen könnte, um damit einen Anschlag vorzubereiten".

Gemäß Bäcker lässt das Polizeigesetz zudem Videoüberwachung überall dort zu, „wo erhebliche Gefahren für die öffentliche Sicherheit zu entstehen drohen". Es sei nicht nötig nachzuweisen, „dass sich bestimmte Orte etwa in ihrer Kriminalitätsbelastung vom übrigen öffentlichen Raum abheben". So werde „im Ergebnis eine flächendeckende Überwachung möglich". Problematisch sei auch, dass in einem Streifen von 30 Kilometern Breite entlang der Staatsgrenzen alle VerkehrsteilnehmerInnen mit „intelligenter" Videotechnik überwacht werden könnten, was eine automatisierte Gesichtserkennung einschließe. Für die „ausufernde Datenspeicherung bei der Polizei" gebe es kaum Grenzen. Schon wer sich „zur falschen Zeit am falschen Ort" etwa in der Nähe einer Demonstration aufhalte, könnte auf Dauer in polizeilichen Datensammlungen landen. Langfristig könnte so „ein umfassender Katalog der Bevölkerung" entstehen. Die Kläger zielen zudem auf Zwangsmaßnahmen wie Aufenthaltsgebote, Kontaktsperren oder elektronische Fußfesseln gegen „Gefährder" ab. Falsche Prognosen könnten hier Bäcker zufolge „zu selbsterfüllenden Prophezeiungen werden, aus denen es kein Entrinnen gibt".

Mit der Novelle können künftig auch Scanner für den automatisierten Abgleich von Kfz-Kennzeichen an sächsischen Straßen verstärkt eingesetzt werden. Spezialeinheiten etwa zur Terrorabwehr sollen in besonderen Einsatzsituationen auf Waffen mit hoher Reichweite und Durchschlagskraft wie Maschinengewehre oder Handgranaten zurückgreifen dürfen. Grüne und Linke wollen mit dem Verfahren den mit der Reform ihrer Ansicht nach verknüpften „Frontalangriff auf die Bürgerrechte" stoppen. Es ist vorgesehen, dass das Gesetz am 01.01.2020 in Kraft tritt. Eine

Entscheidung des Gerichts wird erst Ende 2020 erwartet (Krempl, Überwachung: Linke und Grüne klagen gegen neues sächsisches Polizeigesetz, www.heise.de 12.08.2019, Kurzlink: https://heise.de/-4495071).

Sachsen

Grünen-Wahlkampf-App „problematisch"

Die anlässlich des Landtagswahlkampfes eingesetzte Wahlkampf-App von Bündnis 90/Die Grünen wird in Bezug auf den Datenschutz als bedenklich eingestuft. Eine anlässlich der Wahl in Sachsen im Auftrag des MDR durchgeführte Analyse der Hochschule Mittweida, die die Wahlkampf-Apps der Parteien untersuchte, ergab, dass insbesondere die App der Grünen datenschutzrechtliche Probleme birgt. Damit wird erfasst, ob eine Haustür geöffnet wurde, wie die Reaktion war sowie die Wahl-Wahrscheinlichkeit. Weil mit der App GPS-Standortdaten erfasst und gespeichert werden können, sind die erhobenen Daten einer Person zuzuordnen. Dies gilt vor allem in Gebieten mit wenigen Häusern und AnwohnerInnen.

Dirk Pawlaszczyk, Professor für Cyber-Sicherheit an der Hochschule Mittweida, kommt in seinem Testbericht zu dem Schluss: „Die Wahlkampf-App der Grünen ist in Punkto Datensicherheit und Datenschutz als bedenklich einzustufen." Ohne die ausdrückliche Zustimmung der Betroffenen sei eine solche Form der Datenerhebung aus Sicht des Datenschutzes problematisch. Die Grünen bestätigten die Erhebung der GPS-Standortdaten. Das diene, so eine Sprecherin, lediglich der Dokumentation, welches Haus bereits besucht wurde. Nach der Datenübertragung auf den Server würde die politische Einstellung der angetroffenen Person anonymisiert gespeichert. „Die Wahlkampf-App befindet sich noch im Probelauf. Nach dem Sommer werden wir sie evaluieren." Ein Personenbezug besteht jedoch laut Pawlaszczyk weiterhin, da die App sämtliche Einträge erst lokal auf dem Handy speichert, bevor sie sie weitergibt. Die Zwischenspeicherung auf dem Handy stelle ein zusätzliches Sicherheitsrisiko dar. Politische Ansichten sind gemäß der Datenschutz-Grundverordnung als besonders sensitiv anzusehen und stehen deshalb unter einem besonderen Schutz.

Bereits in der Vergangenheit hatten Wahlkampf-Apps für Probleme gesorgt. Im Bundestagswahlkampf der CDU 2017 ließ auch deren App einen Rückschluss auf den Wohnort der Befragten zu. Die Berliner Datenschutzbeauftrage veranlasste eine Löschung aller Daten, bei denen eine Anonymisierung nicht gewährleistet werden konnte. Die CDU besserte daraufhin nach und erfasst heute nicht mehr den genauen Standort. Daher stuft die aktuelle Analyse der Hochschule Mittweida die CDU-App bei Datenschutz und Datensicherheit als „gut" ein. Ebenso lautet das Fazit für die Anwendung der SPD.

Die Hochschule hat die Wahlkampf-Apps der CDU, SPD sowie der Grünen technisch ausgewertet. Die App der Partei Die Linke wird gemäß den vorliegenden Informationen derzeit nicht genutzt. Diese sei laut Landesverband Sachsen noch nicht auf dem Stand, dass sie flächendeckend eingesetzt werden könnte. Andere Parteien besitzen keine derartigen Apps für den Wahlkampf. Die Grünen und die CDU setzten ihre App im Wahlkampf in Sachsen ein (Sauer, GPS-Daten werden gespeichert Datenschützer stuft Wahlkampf-App der Grünen als „bedenklich" ein, www.focus.de 14.08.2019).

Sachsen-Anhalt

Verfassungsschutz soll online spionieren dürfen

Sachsen-Anhalt will sein Verfassungsschutzgesetz der technischen Entwicklung anpassen und den beamteten Verfassungsschützern erlauben, verschlüsselte Kommunikation mitzuverfolgen, wenn ein Richter zustimmt. Verfassungsschutzchef Jochen Hollmann warb für seine Forderung: „Wir haben die gesetzlichen Regeln so angepasst, dass wir im Grunde genommen weiter das machen können, was wir schon immer machen durften, bevor das Internet kam, bevor Verschlüsselungstechniken kamen. Wir sind mit der Zeit – und so ging es ja vielen Nachrichtendiensten und der Polizei – immer weniger in der Lage gewesen, Gespräche auch inhaltlich abzuhören." Hollmann betonte, die sogenannte Quellen-TKÜ sei auf den absoluten Ausnahmefall beschränkt, vielleicht ein oder zwei im Jahr. Der Verfassungsschutz sei dafür auch auf das Bundesamt für Verfassungsschutz angewiesen. Es gehe um jede laufende Kommunikation vom Telefonat bis zu Messenger-Diensten.

Sachsen-Anhalts neues Gesetz sieht zudem vor, dass Erkenntnisse über 14- und 15-Jährige nicht nur gespeichert, sondern auch an den Verfassungsschutzverbund weitergegeben werden können. Bislang würden Daten in jeweils zweistelliger Zahl gespeichert, sagte Hollmann. Als Beispiel nannte er 15-Jährige, die zur Terrormiliz IS ausgereist sind. Wenn beim Bund oder in anderen Ländern Erkenntnisse aufliefen, könnten die aus Sachsen-Anhalt dazu gespeichert werden. Das sei wichtig für eine gemeinsame Sicherheitsarchitektur in Deutschland, ergänzte Innenminister Holger Stahlknecht (CDU).

Im Gesetzentwurf werden die nachrichtendienstlichen Mittel für die verdeckte Informationsbeschaffung aufgezählt, etwa die Observation, der Einsatz von Vertrauenspersonen und verdeckten Ermittlern, Bild-Aufzeichnungen, verdeckte Ermittlungen mit und ohne Technik, Tarnpapiere und Tarnkennzeichen und das Aufklären des Internets. Alles, was nicht aufgezählt sei, gehe, so Verfassungsschutzchef Hollman, auch nicht. Neu sei auch eine stärkere parlamentarische Kontrolle des Verfassungsschutzes. Bei zwei Beratungen des Parlamentarischen Kontrollgremiums sei ein öffentlicher Teil vorgesehen. Bisher ist die Öffentlichkeit komplett ausgeschlossen. Das Gremium hieß bislang Parlamentarische Kontrollkommission (PKK) und heißt künftig Parlamentarisches Kontrollgremium (PKG), weil für die verbotene Arbeiterpartei Kurdistans ebenfalls die Abkürzung PKK genutzt wird. Das Gesetz muss vom Landtag beschlossen werden (Verfassungsschutzgesetz: Sachsen-Anhalt will Staatstrojaner einsetzen, www.heise.de 13.08.2019; Kurzlink: https://heise.de/-4496108).

Datenschutznachrichten aus dem Ausland

Weltweit

Biometrische Zugangssicherungsdaten im Netz verfügbar

Die südkoreanische IT-Firma Suprema bezeichnet sich selbst als Marktführer in Europa und in asiatischen Ländern bei biometrischen Zutrittskontrollsystemen. Die Firma erlebte nun ihren Sicherheitsgau mit ihrer Biometriedatenbank „Biostar 2“: Forschende des israelischen Online-Dienstes vpnMentor haben entdeckt, dass das webbasierte System mit hochsensiblen personenbezogenen Informationen weitgehend ungeschützt am Internet hing. Die Experten konnten sich nach eigenen Angaben ohne große Mühen Zugang zu 27,8 Millionen Einträgen verschaffen, die 23 Gigabyte an Daten ausmachten. Darunter waren neben unverschlüsselten Profilinformationen wie Nutzernamen und Passwörtern über eine Million Fingerabdrücke sowie eine ungenannte Zahl an Gesichtsbildern. Biostar 2 verwendet Fingerabdrücke oder Gesichtsscans auf einer Online-Plattform für intelligente Türschlösser, mit der Unternehmen die Zugangskontrolle etwa für ihre Niederlassungen oder Lagerhallen selbst organisieren können. Erst zuvor hatte Suprema eine Kooperation mit dem niederländischen Elektrokonzern Nedap abgeschlossen, der IT-Ausrüstung für die Warensicherung, Zutrittskontrollen, RFID und Wahlcomputer herstellt. Seitdem ist Biostar 2 in das noch größere System AEOS zur biometrischen Zugangskontrolle integriert, das über 5.700 Organisationen in 83 Ländern nutzen. Darunter befinden sich gemäß Presseberichten Konzerne genauso wie kleine Betriebe, Regierungseinrichtungen, Banken und die britische Metropolitan Police.

Das von den Datenschutzforschern Noam Rotem und Ran Locar angeführte Team entdeckte die massive Schwachstelle im Rahmen eines großen Projekts, mit dem die Hacker mit einfachen Portscans quasi an den Türklinken von Webservern rütteln und testen, ob sie aufgehen. Finden sie offene Stellen, suchen sie darüber nach weiteren, tiefer in die Systeme führenden Angriffspunkten. Bei Biostar 2 gelang es den Experten, die Datenbank über einen gängigen Web-Browser anzusprechen. Durch die Manipulation der Suchkriterien für die Webadresse stießen sie auf die brisanten großen Datenmengen. Neben den biometrischen Merkmalen fanden sie etwa Protokolle über den Zugang zu den angeschlossenen Einrichtungen sowie Sicherheitsstufen und -freigaben nebst persönlichen Daten des Personals.

In Deutschland sollen Daten von Identbase betroffen gewesen sein, einem Ausrüster von Ausweis- und Zugangskontrollkarten. Böswillige Hacker hätten sich so einen kompletten Zugang zu Administratorkonten verschaffen und die gesamten restlichen Sicherheitseinstellungen ändern, also auch etwa bestimmte Personen aus Räumen ausschließen können. Kriminelle könnten in Echtzeit verfolgen, welcher Benutzende welche Einrichtung oder welches Büro betreten. Ferner wäre es ihnen etwa möglich gewesen, Datensätze in den Firmenkonten neu anzulegen und zu manipulieren. Die gesamte biometrische Sicherheitsinfrastruktur eines Gebäudes würde so nutzlos und hinfällig.

Die Sicherheitsexperten warnen, dass die Lücke Erpressungen sowie massiven Identitätsdiebstahl und darauf basierenden Betrug wie Phising erleichtern könnte. Sollten Fingerabdrücke gestohlen worden sein, könnten diese für vielfältige Zwecke missbraucht werden. Dies wiege besonders schwer, da biometrische Merkmale im Gegensatz etwa zu Passwörtern nicht mehr verändert werden und damit auf Dauer kompromittiert seien. Ob sich andere Hacker bereits unbemerkt Zugang zu dem Datenfundus verschafft haben, ist unklar. Rotem und sein Team haben Biostar am 07.08.2019 auf die Schwachstellen hingewiesen, wobei sie Angestellte in Deutschland zunächst zurückgewiesen hätten. Erst nach der Ansprache einer französischen Zweigstelle sei die Lücke am 13.08.2019 geschlossen worden.

Entsetzt zeigten sich die Forschenden, dass Suprema die vollständigen biometrischen Daten in dem System abspeicherte. Dem Stand der Technik hätte es entsprochen, nur Hashwerte etwa von Fingerabdrücken aufzubewahren, die nicht einfach kopiert und frei verwendet werden könnten. Überrascht waren sie zudem, dass auch viele Kunden der Koreaner für ihre Konten nur Standardkennungen wie „Passwort“ oder „abcd1234“ verwendeten. Supremas Marketingchef Andy Ahn erklärte, dass sein Unternehmen die von vpnMentor gelieferten Informationen eingehend prüfe. Sollte eine andauernde Bedrohung bestehen, werde es umgehend handeln und die KundInnen informieren (Krempl, Biometriedatenbank mit 27,8 Millionen Einträgen ungesichert im Netz, www.heise.de 14.08.2019, Kurzlink: https://heise.de/-4496575).

Italien

Datenhack bei Unicredit

Unbekannte Kriminelle haben rund drei Millionen Namen, Mailadressen und Telefonnummern von KundInnen der italienischen Bank Unicredit erbeutet. Betroffen sei eine Datei, die im Jahr 2015 erstellt worden sei und ausschließlich italienische Datensätze beinhalte. Dies teilte das Unternehmen am 28.10.2019 in Mailand mit. Die Kombination solcher Daten ermöglicht es Online-Kriminellen, KundInnen so genannte Phishing-E-Mails zu schicken, mit denen sie ihnen über präparierte Links zum Beispiel Passwörter abschwindeln können. Unicredit betonte, viel zu tun, um solche Hacks zu verhindern. In den Bereich der IT-Sicherheit seien seit 2016 insgesamt 2,4 Milliarden Euro investiert worden. Hierzu gehöre auch eine neue Nutzeridentifikation, die 2019 an den Start ging. Sie soll den Zugriff via Internet und Smartphone-App sicherer machen (Unicredit: Daten erbeutet, SZ 29.10.2019, 26).

Italien

Salvini ließ Sinti/Roma erfassen

Der rechtsradikale frühere italienische Innenminister Matteo Salvini ließ, kurz bevor er wegen einer Regierungsumbildung seinen Posten verlor, „Lager“ der Minderheit der Sinti und Roma erfassen. Sein Ministerium forderte im Juli 2019 die italienischen Präfekten auf, innerhalb von zwei Wochen Berichte über Roma, Sinti und andere „fahrende Leute“ vorzulegen. Die Maßnahme galt als Vorbereitung für großangelegte Abschiebungen. Salvini, der den Plan schon 2018 angekündigt hatte, sorgte damit nicht nur bei MenschenrechtlerInnen für Empörung. Der Vizepräsident des Internationalen Auschwitz Komitees, Christoph Heubner, reagierte hierauf wie folgt: „Mit seinen erneuten Drohungen gegen Sinti und Roma stößt Salvini die Türen des Hasses in Italien weit auf und setzt erneut die Schwächsten der Schwachen in Europa dem Hass der Straße aus, den er selber bei seinen Anhängern immer wieder hervorkitzelt. Alle diese Strategien des Hasses sind Europas unwürdig“. Die Erfassung von Minderheiten hat eine lange und menschenverachtende Geschichte, gilt sie doch als erster Schritt für weitere Diskriminierungen, Maßnahmen und in manchen Fällen sogar Vernichtung. In Deutschland gipfelte die Erfassung im Porajmos, dem Genozid an Sinti und Roma (Reuter, Erfassung der Roma in Italien: „Salvini stößt Türen des Hasses weit auf“, netzpolitik.org, 18.07.2019).

Schweiz

DNA-Profiling bei Klima-AktivistInnen

Mitte Juli 2019 demonstrierten Klima-AktivistInnen vor den Großbanken UBS und Credit Suisse. Sie verbarrikadierten in Basel und Zürich die Eingänge zu den Banken. Rund 83 Personen wurden verhaftet, 48 Stunden lang eingesperrt und sie müssen zusätzlich hohe Bußen bezahlen. Die Polizei nahm Speichelproben und erstellt nun DNA-Profile. Die Speichelproben wurden gegen ihren Willen entnommen. Unter den Festgenommenen befanden sich auch Minderjährige.

Gemäß dem schweizerischen Recht müssen DNA-Proben nach spätestens 90 Tagen wieder aus dem System gelöscht werden. DNA-Profile zu erstellen ist eine noch heiklere Angelegenheit. Die Basler und die Zürcher Staatsanwaltschaften haben in diesem Fall spezielle Verfügungen ausgestellt. Reto Müller, Lehrbeauftragter für Sicherheits- und Polizeirecht an der Universität Basel, kommentierte: „DNA-Proben greifen in das Grundrecht der informationellen Selbstbestimmung ein. Bei gewaltfreien politischen Demonstrationen sind solche nicht verhältnismäßig“. Die Staatsanwaltschaften bestätigten die Maßnahme, gaben aber hierzu keine Erklärung ab. Es wird vermutet, dass die DNA-Profile genutzt werden sollen, um vergangene und zukünftige Vergehen aufklären zu können. Die Organisation Kollektiv Climate Justice erklärte: „Mit den DNA-Entnahmen machen sich Polizei und Staatsanwaltschaft zu Handlangern der Banken.“ Die Klima-AktivistInnen kündeten den Gang vor die Gerichte an. Sie würden, falls es notwendig sein sollte, das Verfahren bis vor den europäischen Gerichtshof für Menschenrechte bringen (Polizei erstellt DNA-Profile von Klima-Aktivisten, telebasel.ch 21.07.2019).

Europaweit

Datenschützerin warnt vor „Facebook Dating“

Facebook hat für 2020 in Europa als neuen Dienst „Dating“ angekündigt, ein Dienst, der in den USA schon nutzbar ist. Dabei handelt es sich um eine datengetriebene Partnervermittlung. Als Daumenregel gilt dabei, dass Personen gut zueinander passen, wenn sie gemeinsame Interessen haben und psychologisch auf einer Wellenlänge zu sein scheinen. Viele Facebook-Nutzende geben dem Unternehmen ihre Interessen preis, außerdem führt es detaillierte Analysen durch, um passgenaue Werbung zu ermöglichen. Im Grunde ist es egal, ob Produkte an die passenden Kunden vermittelt oder Partner zusammengebracht werden sollen: Hilfreich für beides sind psychologische Profile.

Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein und Leiterin des Unabhängigen Landeszentrum für Datenschutz (ULD), warnte vor dem angekündigten Dienst: „Für Facebook ist die Analyse von psychologischen Eigenschaften und anderen sensiblen Informationen kein Neuland: 2017 wurde bekannt, dass ein australischer Forscher bei Facebook Algorithmen entwickelte, um festzustellen, ob sich die jugendlichen Nutzerinnen und Nutzer ängstlich, nervös, gestresst, dumm, unsicher, wertlos oder als Versager fühlten. Vor einem Jahr lieferte Facebook gezielt ‚Gay-Cure‘-Werbung an homosexuelle junge Leute aus – solche Werbung erklärt, wie sie vermeintlich von ihrer sexuellen Präferenz ‚geheilt‘ werden können, und vermittelt den Eindruck, es sei mit einem etwas nicht in Ordnung. Erst nach einem Hinweis der Medien wurden diese manipulativen Werbungen gestoppt. Außerdem verwendet Facebook laut Medienberichten in einigen Ländern Verfahren der Künstlichen Intelligenz, um Gemütszustände anhand von Postings oder Fotos – bis hin zu Depressionen oder Suizidgefahr – zu erkennen.“

Bei Facebook Dating würden die interessierten Nutzenden ausgefragt, um auf dieser Basis passende PartnerInnen zu vermitteln. In einer „Secret-Crush“-Liste kann man eintragen, für welche der Freunde man heimlich schwärmt. In den Nutzerfragen geht es z. B. um Angaben zu dem, was man leidenschaftlich gern tut, wofür man dankbar ist, welches Ziel man noch nicht erreicht hat oder was man gar nicht kann. Hansen dazu: „Das sind schon etwas tiefergehende Persönlichkeitsfragen, die es ermöglichen, eine Person mit ihren Facetten näher kennenzulernen – ebenso für interessierte Vermittlungskandidaten wie für Facebook selbst. Werden diese Informationen künftig die Basis für zielgerichtete Werbung sein? Es wäre leicht möglich, die selbst offenbarten oder vom Algorithmus entdeckten Unsicherheiten und Schwächen von Personen auszunutzen – dann wäre einer Manipulation der Menschen Tür und Tor geöffnet.“

Der Dating-Dienst kann dazu führen, dass die Nutzenden Facebook weitere Daten zur Verfügung stellen, z. B.

Standortdaten, die für das Verkuppeln ausgewertet werden können, oder Inhalte des eigenen Instagram-Nutzerkontos, die sich dort integrieren lassen. Hansen: „Facebook hat schon jetzt eine Riesenmenge an Informationen über die Nutzer – einschließlich Interessen und psychologischer Einschätzungen. Mit der Dating-Funktion werden es noch deutlich mehr werden. Die Skandale der letzten Monate und Jahre um Facebook haben aber deutlich gezeigt, dass die Plattform immer wieder große Sicherheits- und Datenschutzmängel hat. Erst vor wenigen Tagen wurde die Entdeckung eines Datenbestands mit 419 Millionen Einträgen zu Facebook-Nutzer-IDs und Telefonnummern bekannt, der frei im Internet verfügbar war. Wenn Nutzerdaten bei Facebook nicht sicher sind, fehlt mir das Vertrauen, dass das Unternehmen die sensiblen Dating-Informationen gut genug schützen wird. Sonst tauchen bald die ersten Datenbestände mit ‚Secret-Crush'-Listen oder psychologischen Profilen zu Facebook-Mitgliedern im Internet auf. Mein Rat: Daten zur Partnersuche nur datenschutzkonformen und vertrauenswürdigen Diensten ohne Sicherheitsprobleme anvertrauen – Finger weg vom Facebook-Dating und anderen Anbietern ohne ausreichenden Schutz" (ULD PM, Facebook-Dating – aus Datenschutzsicht ein klarer Abtörner, 07.09.2019).

Griechenland

PwC erhält sechsstellige Strafe für DSGVO-Verstoß

Die griechische Niederlassung des renommierten Wirtschaftsprüfungs- und Steuerberatungsunternehmens PricewaterhouseCoopers (PwC) erhielt nach einer Beschwerde von der dortigen Datenschutzbehörde wegen eines Verstoßes gegen die Rechtmäßigkeit der Datenverarbeitung ein Bußgeld in Höhe von 150.000 €, da von den Mitarbeitenden für die Verarbeitung ihrer Personaldaten Einwilligungen eingeholt wurden. Die griechische Behörde wertete dies als Verstoß gegen die Grundsätze der Datenverarbeitung, da den Mitarbeitenden so das Gefühl vermittelt wurde, dass sie in die Datenverarbeitung einwilligen müssten, was jedoch nicht der Fall ist. Beschäftigtendaten werden überwiegend auf Grundlage rechtlicher Pflichten sowie des Arbeitsvertrags verarbeitet. In Sonderfällen greife das berechtigte Interesse des Arbeitgebers. Die Einwilligung wird im Arbeitsverhältnis stets als kritisch eingestuft, da aufgrund des hierarchischen Verhältnisses zwischen Arbeitgeber und Arbeitnehmer selten von echter Freiwilligkeit ausgegangen werden kann. Die griechische Datenschutzbehörde betrachtete den Umstand, dass PwC für diese Datenverarbeitung Einwilligungserklärungen unterschreiben ließ, als Verstoß gegen die Rechtmäßigkeit der Datenverarbeitung und trug dem Unternehmen auf, die korrekten Rechtsgrundlagen zu wählen und dies den Beschäftigten auch mitzuteilen (DSG-Service 2019, www.secur-data.at/fileadmin/Downloads/DSGI2019-92.pdf, S. 4).

Schweden

Bußgeld gegen Schule wegen automatischer Gesichtserkennung

Mit einem Bußgeld von umgerechnet rund 18.000 € (200.000 SEK) endete in einer schwedischen Schule in Skellefteå ein Pilotprojekt, in dem diese die Anwesenheit von SchülerInnen mittels Gesichtserkennung kontrollierte. Statt eines üblichen Anwesenheitsbuches wurden 22 SchülerInnen über den Zeitraum von 3 Wochen mittels Gesichtserkennung im Unterricht überwacht. Hierfür holte die Schule die Einwilligung der Betroffenen ein. Die schwedische Datenschutzbehörde entschied aber, dass dies unzulässig sei und zog die Wirksamkeit der Einwilligungen in Zweifel, da diese in einem hierarchischen Verhältnis selten haltbar sei. Verarbeitet wurden biometrische Daten, weshalb nach Art. 9 DSGVO eine ausdrückliche Einwilligung eingeholt werden musste. Unter Berücksichtigung des Abhängigkeitsverhältnisses und der Tatsache, dass für die Überprüfung der Anwesenheit auch andere, geringere Mittel als die biometrische Erfassung der Gesichter angewendet können, waren gemäß der Aufsichtsbehörde sowohl die Datenanwendung als auch die Einwilligung die falsche Wahl. Anders als in Deutschland ist es in Schweden möglich, Bußgelder gegen öffentliche Stellen zu verhängen (DSG-Service 2019, www.secur-data.at/fileadmin/Downloads/DSGI2019-92.pdf, S. 4 f.).

USA

Konzerne fordern nationales Datenschutzrecht

51 große US-Konzerne fordern ein einheitliches Verbraucher-Datenschutzgesetz für die gesamten USA. Bisher gibt es das in dem Land mit dem COPPA (Children`s Online Privacy Protection Act) nur für Personen jünger als 13. Seit den Wahlen 2018 ist eine neue Politik-Generation tätig, die in mehreren US-Staaten Datenschutzgesetze auf den Weg gebracht hat. Marc Rotenberg vom Electronic Privacy Information Center (EPIC) hofft nun, dass die neue Machtverteilung zwischen Republikanern und Demokraten zur Kontrolle des Datenhungers von Geheimdiensten und Privatfirmen führt. Die Konzerne wollen sich nicht mit über 50 verschiedenen Gesetzen und Behörden herumschlagen und fordern deshalb ein Bundesgesetz ohne Anspruch auf gerichtliche Durchsetzung.

In dem am 10.09.2019 veröffentlichten Brief von 51 Konzernchefs an die RepräsentantInnen und SenatorInnen des US Kongresses sorgen sich die Verfasser um das Vertrauen ihrer KundInnen und drängen den Gesetzgeber zur Eile: „Wir können und sollen von Verbrauchern nicht erwarten, dass sie die Regeln verstehen, die sich abhängig davon ändern können, in welchem Staat sie wohnen, in welchem Staat sie ins Internet gehen und in welchem Staat der (Unternehmer) sitzt". Die Zersplitterung in Staaten-Gesetze bedrohe die „Innovation und globale Wettbewerbsfähigkeit" der USA. Zu den Unterzeichnern des Schreibens zählen neben Netzbetreibern, Geldinstituten und Kfz-Herstellern auch Unternehmen wie Amazon, Dell, Harman, IBM, Motorola Solutions, Qualcomm, Salesforce und SAP. Sie stecken auch gleich einen Rahmen ab, den sie „Framework for Consumer Privacy Legislation" nennen, in dem die Interessen der Konzerne zum Aus-

druck kommen: Die USA sollen als Vorreiter für Datenschutz dargestellt werden, um das Vertrauen der VerbraucherInnen zurückzugewinnen. Einheitliche Regeln innerhalb der USA über alle Branchen hinweg sollen die Kosten senken, für kleine Unternehmen soll es Ausnahmen geben. Staaten und Kommunen sollen keine Datenschutzregeln mehr erlassen können. Gefordert wird auch, dass Daten friktionsfrei über internationale Grenzen fließen dürfen.

In der allerletzten Zeile des Dokuments wird ihm der Zahn gezogen: Betroffene sollen ausdrücklich kein Recht haben, bei Datenschutzverletzungen zu Gericht zu gehen und z. B. Schadenersatz zu erstreiten. Für die Durchsetzung des gewünschten Verbraucher-Datenschutzgesetzes soll vielmehr die Handelsbehörde Federal Trade Commission (FTC) zuständig sein. Zudem dürften die Justizminister der einzelnen US-Staaten klagen, jeweils für EinwohnerInnen ihres Staates. Die FTC ist ein politisch besetztes Gremium, das sich auf symbolträchtige Verfahren mit hohen Strafen gegen einzelne Unternehmen spezialisiert hat. Das sorgt für Schlagzeilen, hat aber wenig mit breiter Rechtsdurchsetzung zu tun. Betroffene haben keinen Anspruch auf ein FTC-Verfahren. Sie können behördliches Eingreifen lediglich anregen, was in den seltensten Fällen Erfolg hat.

Die geringe Datenschutz-Wirkung der FTC zeigt sich am COPPA. Dieses Gesetz ist rund 20 Jahre alt, wird aber weitgehend ignoriert. 2018 stellte eine Untersuchung fest, dass in Googles Play Store drei Viertel aller Kinder-Apps gegen COPPA verstoßen. Soweit bekannt, hat die FTC seither gerade einmal vier Unternehmen belangt: Musical.ly (TikTok) musste 5,7 Mio. US-Dollar Strafe zahlen (DANA 3/2019, 165), YouTube 170 Millionen. Eine Webseite ist mit 35.000 Dollar davongekommen, eine weitere mit dem Versprechen, sich zu bessern. Zudem wurden drei Dating-Apps aus dem Play Store entfernt. Auch die Hoffnung auf Klagen der Justizminister der einzelnen Staaten sind trügerisch, da diese Ämter politisch besetzt werden, meistens durch direkte Wahl. Betroffene können ihren Justizminister auch nicht dazu zwingen, gegen Rechtsbrecher vorzugehen oder einen schlechten Vergleich verhindern.

Die Konzerne schlagen vor, dass VerbraucherInnen Anspruch auf „angemessenen" (reasonable) Zugang zu verständlichen Angaben über den Datengebrauch ihrer Vertragspartner erhalten. Außerdem sollen sie „angemessen" Kontrolle über Sammlung und Nutzung ihrer Daten ausüben können. Hinzukommen soll die Gelegenheit, über den Verkauf ihrer Daten an Dritte „auszuwählen". Für kostenlose Datenweitergabe wird das nicht gefordert. Unternehmen sollen jene Dritten, denen sie Verbraucherdaten zukommen lassen, vertraglich dazu verpflichten, Datenschutz-Entscheidungen der VerbraucherInnen zu respektieren. Verantwortung für die Einhaltung dieser Verpflichtung soll aber ausschließlich beim Dritten liegen, nicht bei der Datenquelle. Und die Dritten sollen ausdrücklich nicht verpflichtet werden, Auskunft über Datensammlung und -verwendung zu geben.

Zudem erwähnt der Vorschlag ein Recht auf Datenlöschung. Es ist mit umfangreichen Ausnahmen konzipiert. Beispielsweise soll es keinen Löschanspruch geben, solange die Daten noch für „legitime Geschäftszwecke", freie Meinungsäußerung oder „Information" benötigt werden. Und wenn die Löschung aufgrund der Art und Weise der Speicherung aufwändig wäre, soll es hinreichen, die Daten „außerhalb praktischer Anwendung" zu stellen. Jeder Datenverarbeiter soll selbst entscheiden, was angemessen ist, abhängig von der Art der gespeicherten Information und dem empfundenen Risiko. Von Datenschutz für Beschäftigte, Einzelunternehmer oder Auszubildende ist in dem Framework keine Rede. Gegenüber Behörden soll das Gesetz explizit nicht gelten. Es wird ausschließlich für die Beziehung zwischen Unternehmen und Verbrauchern in ihrer Eigenschaft als solche gewünscht (Sokolov, US-Konzerne fordern Datenschutzgesetz – aber bitte zahnlos, www.heise.de 11.09.2019, Kurzlink: https://heise.de/-4519541).

USA

Facebook prüft und sperrt Apps

Facebook hat gemäß eigenen Unternehmensangaben im Zuge der Untersuchungen zum Skandal um die Datenanalysefirma Cambridge Analytica rund 69.000 Apps auf seiner Plattform blockiert. Gemäß Unterlagen aus einem Gerichtsverfahren in Boston erfolgte dies bei den meisten Apps vorsorglich, ohne klären zu können, ob sie tatsächlich Nutzerdaten missbraucht haben. Insgesamt sind Apps von rund 400 Entwicklern betroffen.

Ein Großteil der Apps wurde demnach blockiert, weil ihre Entwickler bei der Untersuchung des Online-Netzwerks nicht kooperieren wollten und auf per E-Mail versandte Fragen nicht reagierten. Bei ca. 10.000 Apps prüft Facebook, ob Regeln zum Umgang mit Daten der NutzerInnen verletzt wurden. Sie zeigten „Charakteristika, die mit höherem Risiko von Datenmissbrauch einhergehen". 6.000 Anwendungen gerieten in den Fokus, weil sie von vielen Nutzenden installiert wurden. Bei 2.000 habe Facebook vertieft die Entwickler überprüft und bei weiteren 2.000 schaute sich das Online-Netzwerk an, ob sie zu viele Nutzerinformationen abgefragt hätten.

Die Zahlen wurden im Zuge einer Untersuchung Facebooks durch die Staatsanwaltschaft des US-Bundesstaats Massachusetts bekannt. Ein Gericht lehnte den Antrag von Facebook ab, sie unter Verschluss zu halten. Die Staatsanwälte wollten auch gern wissen, wer die betroffenen App-Entwickler sind; Facebook hält die Informationen, so Presseangaben, aber zurück. Der Staatsanwaltschaft in Boston zufolge hatte Facebook bereits 2014 Entwicklern gestattet, mindestens 9 Mio. Apps in das Netzwerk zu integrieren. Jahrelang sei erlaubt worden, Nutzungsdaten zu sammeln, darunter Fotos, Beschäftigungsverhältnisse, Geburtsdaten und Likes. Dies betraf nicht nur Personen, die die Apps installiert hatten, sondern auch deren Facebook-Freunde. Aus den Gerichtsunterlagen geht hervor, dass Facebook rund 2 Mio. Apps identifiziert hat, die wegen möglichen Missbrauchs von Nutzungsdaten genauer untersucht werden sollten. Facebook hat nach eigenen Angaben bislang Millionen von Apps kontrolliert.

Der Fall Cambridge Analytica brachte Facebook im Frühjahr 2018 massiv unter Druck. Daten von Facebook-Nutzenden waren vom Entwickler einer Umfrage-App vor über fünf Jahren widerrechtlich

an Cambridge Analytica weitergegeben worden. Mit den Informationen wurde versucht, die US-Präsidentschaftswahlen 2016 zu beeinflussen, die Donald Trump gewann. Facebook wusste mindestens seit 2016 von dem Fall, begnügte sich aber mit der Zusicherung, dass die Daten vernichtet worden seien und informierte die NutzerInnen nicht. Facebook-Chef Mark Zuckerberg musste deshalb vor dem Kongress aussagen. Die Untersuchung des Falls durch die US-Aufsichtsbehörde FTC führte zu einer Strafe von 5 Mrd. Dollar für Facebook (vgl. DANA 3/2019, 164 f.; Facebook sperrte Zehntausende Apps, www.spiegel.de 21.09.2019).

USA

Ring macht Video-Sicherheits-Deal mit Polizei

Die Amazon-Tochter Ring vertreibt in den USA eine vernetzte Türklingel mit Überwachungskamera, Bewegungsmelder, Mikrophon und Lautsprecher. Zur Vermarktung bedient sich der Konzern mindestens 200 Polizeibehörden quer durchs Land, wie aus bisher geheimen Unterlagen bekannt wurde. Diese sollen ihren BürgerInnen Ring-Produkte und die passende App „Neighbors“ empfehlen. Bei Erfolg winken ihnen Überwachungsvideos sowie Guthaben zum Kauf weiterer Ring-Kameras. Das Unternehmen verpflichtete Polizeibehörden zur Geheimhaltung. Laut einer von Ring und der Polizei Lakeland unterzeichneten Absichtserklärung sollte die Firma ein Startpaket von 15 Kameras kostenfrei liefern. Im Gegenzug müssten PolizeibeamtInnen fünf Funktionen wahrnehmen: Ring wünschte sich einen Ansprechpartner für das Projekt, einen Pressesprecher, einen Verantwortlichen für Soziale Netzwerke, einen Beamten zur Koordinierung der mit Ring-Videos unterstützten Untersuchungen sowie einen Verantwortlichen für die Beziehungen zur lokalen Bevölkerung. Ring erklärte, dass PolizistInnen für diese Positionen zur Verfügung zu stellen keine Teilnahmevoraussetzung sei, wogegen in einer gefundenen E-Mail ein Ring-Mitarbeiter die Bestellung der Funktionäre allerdings als „benötigt“ bezeichnete. Für jede im Zuständigkeitsbereich der Polizeibehörde heruntergeladene Neighbors-App sollte die Polizei zehn US-Dollar Gutschrift erhalten, die ausschließlich zum Kauf weiterer Ring-Kameras hätten genutzt werden können. Je nach Modell kosten die vernetzten Türkameras bei Amazon.com aktuell hundert bis zweihundertfünfzig US-Dollar plus Steuern.

Neighbors ist für Ring-Kameras konzipiert, funktioniert aber auch mit vielen Smartphones. Die App erlaubt es, Überwachungsvideos zu veröffentlichen, so dass kooperierende Polizeibehörden und in der Nähe wohnende BürgerInnen die Aufnahmen sehen können. BürgerInnen und Polizei können zudem über Neighbors lokale Sicherheitswarnungen verbreiten. Die Namen und exakten Adressen der Teilnehmenden bleiben laut Ring verschleiert. Zur Unterstützung polizeilicher Untersuchungen können Polizeibehörden, die mit Ring zusammenarbeiten, die BürgerInnen um Freischaltung von Videoaufnahmen ersuchen. Bei freiwilliger Herausgabe können die Ermittler die rechtlichen Schranken für behördlichen Zugriff umgehen. US-Recht verlangt ansonsten eine richterliche Genehmigung, die nur bei konkretem Verdacht ausgestellt werden darf. Lakelands Polizei hat sich schließlich gegen die Kooperation mit Ring entschieden, nicht aus Datenschutzbedenken, sondern weil sie nicht eine bestimmte Marke bewerben will. Doch machen, wie berichtet wird, mindestens 200 US-Polizeibehörden mit, so die Mitschrift eines Lakeland-Polizisten aus einem nicht-öffentlichen Webinar (Sokolov, Private Überwachungskameras: Amazon wollte Vertrieb über Polizei geheim halten, www.heise.de 31.07.2019, Kurzlink: https://heise.de/-4483967).

USA

Bald DNA-Identifizierung von Migranten?

Die US-Regierung will DNA-Proben von MigrantInnen nehmen lassen, die bei der illegalen Einreise festgenommen oder in Internierungslagern festgehalten werden. Die genetischen Informationen sollen in einer Straftäterdatenbank mitgespeichert werden. Wann die neuen Regeln in Kraft treten sollen, und ob sie auch Kinder betreffen würden, die allein die Grenze überqueren, war zunächst nicht bekannt. US-BürgerrechtlerInnen sehen in den Regierungsplänen einen Schritt zur Kriminalisierung von MigrantInnen. Schätzungen zufolge könnten die DNA-Tests längerfristig Hunderttausende Menschen betreffen (DNA-Proben von Migranten, SZ 04.10.2019, 8).

USA

Google trainiert Pixel 4 mit repräsentativen Gesichtsbildern

Google bezahlte Passanten 5 US-$, um ihre Gesichter scannen zu dürfen. Das soll die Gesichtserkennung von Pixel 4 verbessern – die Algorithmen sind sonst nicht ausgewogen. Das Geld gab es nicht bar auf die Hand, sondern in Form eines Geschenkgutscheins. Mit den bezahlten Scans trainierte Google die Gesichtserkennung seines kommenden Pixel-4-Smartphones. Sie ist vergleichbar mit „Face ID“ von Apple, soll laut Google aber flexibler arbeiten. Die „Feldforschung“ in US-Städten soll sicherstellen, dass das Pixel 4 mit vielen unterschiedlichen Gesichtern zurechtkommt. Biometrische Erkennungssysteme hatten in der Vergangenheit immer wieder Schwierigkeiten, Gesichter richtig zu erkennen. Der Grund: Die Algorithmen sind voreingenommen, was Hautfarbe, Geschlecht und Rasse angeht. Amazons Gesichtserkennung Rekognition etwa hat gemäß einer MIT Media Lab-Untersuchung Probleme, weibliche und dunkelhäutige Gesichter zuverlässig zu identifizieren. Eine vorangegangene Studie zeigte auf, dass Algorithmen am besten weiße männliche Gesichter erkennen. Bei dunkelhäutigen Frauen versagte hingegen die Gesichtserkennung. Schuld daran ist eine einseitige Lernbasis. Auch die Web-App „AI Portraits Ars“, die Selfies in Gemälde verwandelte, ignorierte dabei die Hautfarbe der abgelichteten Personen. Aus dunkler Haut wurden in den KI-Gemälden helle, zudem ver-

schwanden asiatische Gesichtszüge. Die KI wurde zuvor mit 45.000 historischen Porträts aus verschiedenen Epochen trainiert – und die zeigen vornehmlich weiße Gesichter. Auch das Lächeln verschwand deshalb aus vielen Selfies, denn damals gab es auf Porträts nichts zu lachen.

Entsprechende Probleme mit einer voreingenommenen Gesichtserkennung will Google bei seinem neuen Pixel-Smartphone unbedingt vermeiden. Mit „Face ID" von Apple besteht starke Konkurrenz. Ziel sei es, so Google, die Gesichtserkennung „mit robuster Sicherheit und Leistung zu entwickeln. Dabei haben wir auch immer die Inklusion im Hinterkopf, damit so viele Menschen wie möglich davon profitieren können." Google will deshalb seinen Algorithmus mit möglichst vielen und vielfältigen Gesichtern trainieren. Apple stellte 2017 für „Face ID" eine „repräsentative Gruppe" an Menschen zusammen, die unterschiedliche Geschlechter, Ethnien und Altersgruppen berücksichtigte. Bei den experimentellen Scans erfasste Google Infrarot-, Farb- sowie Tiefendaten von jedem Gesicht. Zusätzlich werden Zeit, Lichtkonditionen und weitere Zusatzinformationen gespeichert. Ursprünglich hatte Google auch Standortdaten erfasst; diese würden, so Google, aber nicht benötigt und deshalb gelöscht. Jede TeilnehmerIn wurde einer Nummer zugeordnet, separat davon speichert Google die Mailadressen, damit die Gesichtsdaten auf Nachfrage gelöscht werden können. Davon abgesehen werden die Informationen 18 Monate lang gespeichert.

Das kommende Pixel 4 verwendet für die Gesichtserkennung ein ganzes Sensoren-Array, bestehend aus Kamera, Soli-Chip (Radar), Helligkeits- und Distanzsensor sowie zwei Infrarot-Kameras, womit Google für die Erkennung eine komplette Tiefenkarte des Gesichts erstellt. Die Daten speichert das Pixel-Gerät lokal im Sicherheitschip „Titan M". Auf Google-Server gelangen die persönlichen Gesichtsdaten nicht, so Google: Sie „verlassen niemals das Telefon". Pixel 4 soll noch 2019 auf den Markt kommen (Berger, Google zahlt 5 US-Dollar für Gesichtsscan, um Pixel 4 zu trainieren, www.heise.de 30.07.2019, Kurzlink: https://heise.de/-4483351).

Russland

Neue Erkenntnisse über Netzüberwachung durch FSB

Sicherheitsforschende haben eine nicht ausreichend geschützte Datenbank gefunden, in der jede Menge Details über das russische Abhörsystem SORM zusammengetragen waren. Das Cybersecurity-Unternehmen UpGuard hat die Verantwortlichen darauf aufmerksam gemacht, aber darüber hinaus einige der gefundenen Informationen öffentlich gemacht. Demnach werden in Städten überall in Russland auf Betreiben des Geheimdienstes FSB etwa waschmaschinengroße Boxen bei Telefon- und Internetprovidern installiert, mit denen der übermittelte Datenverkehr vollständig erfasst wird.

Im Rahmen der Aufarbeitung des von Edward Snowden öffentlich gemachten NSA-Skandals hatte Anfang 2014 der russische Journalist und Geheimdienstexperte Andrej Soldatow im EU-Parlament erklärt, dass das enthüllte US-Spionageprogramm PRISM jenem aus Russland entspricht. Das sei bereits in der Sowjetunion eingeführt und dann von dem KGB-Nachfolger modernisiert worden. Von UpGuard gefunden wurden ca. 1,7 Terabyte an Daten – darunter 578.000 Fotos –, die ein Mitarbeiter von Nokia nicht ausreichend geschützt habe. Wie das US-Magazin TechCrunch berichtete, enthüllen die Dokumente die Kooperation Nokias beim Ausbau des Massenüberwachungssystems. Der finnische Netzwerkausrüster schlug demnach in den Jahren 2016 und 2017 Änderungen an Russlands Netzen vor, damit sie den Anforderungen der Überwachungsgesetze genügen. Außerdem zeigten die Dokumente, dass die Boxen zur sogenannten „Lawful Interception" direkten Zugriff auf den Datenverkehr haben, der durch die Netze fließt – „inklusive der Telefonate, Nachrichten und Daten". Adressen und Grundrisse würden den genauen Standort aller Überwachungsboxen verraten, jeweils deutlich in rot markiert.

Nokia soll versichert haben, dass es lediglich die Zugänge einrichte, die eigene Technik würde keine durchgeleiteten Daten speichern, analysieren oder verarbeiten. Gemäß TechCrunch erledigt das dann Technik des russischen Herstellers Malvin Systems. Diese ermögliche die Sammlung und Speicherung jeder Menge Daten zu Russlands BürgerInnen und allen, deren Geräte im Mobilfunknetz angemeldet sind. Staatliche angeordnete Überwachung von Kommunikationsnetzen gibt es auch in westlichen Staaten. Alexander Isavnin von der russischen Internet Protection Society hebt hervor, dass die Anbieter die russischen Überwachungsaufforderungen nicht überprüfen, sondern einfach umsetzen müssen: „Nur der FSB weiß, was gesammelt wird". Es gebe keine Kontrolle durch Dritte. (Holland, Russlands PRISM: Datenleck zeigt Nokias Beteiligung an Überwachungsprogramm, www.heise.de 19.09.2019, Kurzlink: https://heise.de/-4533909).

China

Handynummer künftig nur noch nach Gesichtsscan

Von Dezember 2019 an bekommt man in China nur noch einen Internetanschluss oder eine Handynummer, wenn zuvor zur Überprüfung der Identität das Gesicht gescannt wurde. So soll sichergestellt werden, dass hinter dem registrierten Namen die richtige Person steckt. Dass man sich ausweisen muss, wenn man einen Vertrag abschließt, ist in vielen Ländern üblich. Dass dafür Technologie zur Gesichtserkennung eingesetzt wird, ist aber weltweit ein Novum.

Chinas Internetbehörden führen einen unerbittlichen Kampf gegen die Anonymität im heimischen Netz. Bereits heute müssen Internetnutzende sämtliche Accounts bei sozialen Netzwerken und anderen Onlinediensten mit ihrer Handynummer verknüpfen. Sie dient den Behörden als digitale Identifikationsnummer. Fast jede Onlineaktivität kann so im Bruchteil einer Sekunde einer Person zugeordnet werden. Das beginnt bei so banalen Dingen wie dem Eintippen einer Suchanfrage. Das neue Gesetz soll nun auch die letzten Lücken dieses Kontrollsystems schließen. Die digitale Überwachung hat sehr analoge Konsequenzen: Regelmäßig werden Menschen verhaftet,

die sich kritisch gegenüber der Regierung geäußert haben. So wurden jüngst mehrere Personen festgenommen, die angeblich Chinas Flagge online verunglimpft hatten.

Gesichtserkennung ist in China allgegenwärtig. Mittels der Technologie kann man seinen Kaffee oder Rechnungen bezahlen. Universitäten kontrollieren so, wer den Campus betritt. Und mithilfe eines landesweiten Netzwerks aus bald 600 Millionen Kameras werden Menschen auf der Straße identifiziert, die bei Rot über die Straße gegangen sind oder gegen andere Verkehrsregeln verstoßen haben. In einigen Städten werden sie auf Bildschirmen öffentlich angeprangert. Peking wirbt überall auf der Welt für sein hartes Vorgehen im Netz. Das Konzept der sogenannten Cyber-Souveränität soll jeder Regierung das Recht geben, das Internet im eigenen Land nach Belieben zu regulieren und zu zensieren. Dem Thema ist sogar eine eigene, jährliche Internetkonferenz gewidmet.

Im Ausland wird die Technologie kritischer gesehen. Die USA haben jüngst mehrere chinesische Hersteller von Gesichtserkennungssoftware auf eine schwarze Liste gesetzt, weil deren Technologie zur Unterdrückung muslimischer Minderheiten genutzt werden soll. US-Firmen dürfen ihre Technologie nicht mehr ohne Erlaubnis nach China verkaufen. Viele halten die Software zudem schlicht für zu fehleranfällig. Die Folgen sind bisweilen kurios: So soll in China eine Frau nach einer Nasen-OP von keinem System mehr erkannt worden sein. Vor allem nicht von ihrer digitalen Geldbörse, die sie daraufhin nicht mehr zum Zahlen nutzen konnte (Deuber, Überwacht, überall, SZ 19./20.10.2019, 1).

China

Bezahlen mit Gesichts-Biometrie bei WeChat

Face Pay, die Bezahlung per Gesichtserkennung wird in China Realität. Der Messenger-Dienst WeChat hat die Funktion unter dem Namen „Frog Pro“ eingeführt. Die Technik wurde von dem WeChat-Konzern Tencent entwickelt, einem der Big Player im Bezahl-Geschäft: Im Geschäft scannt eine Kamera das Gesicht der KundIn. Die Zahlung wird über die Kontodaten abgewickelt, die sie bei WeChat hinterlegt hat. Das System hat gewaltiges Potenzial. WeChat ist das größte Soziale Netzwerk in Asien. Es verknüpft Funktionen von Facebook, Facebooks Messenger und WhatsApp auf einer Plattform. Allein in China loggen sich täglich 800 Millionen Menschen bei WeChat ein.

Der Hamburgische Datenschutzbeauftragte Johannes Caspar hält die Einbindung biometrischer Daten in den Zahlungsverkehr für gefährlich: „Das Missbrauchspotential ist groß. Es braucht nur ein paar Fotos einer Person, um die gesamte Topologie eines Gesichts zuverlässig rekonstruieren zu können.“ In China werden darüber hinausgehend die Menschen in großem Stil von Kameras überwacht, wenn sie sich in der Öffentlichkeit bewegen. Wer sich zum Beispiel im Straßenverkehr falsch oder fahrlässig verhält, kann Strafpunkte kassieren. Wenn das Bildmaterial aus den flächendeckenden Kameras in falsche Hände geriete, könnten Betrüger mit fremden Identitäten bezahlen.

Selbst die modernste Software zur Gesichtserkennung ist fehleranfällig. Aktuelle Zahlen dazu präsentierten Experten im Mai 2019 beim Internationalen Workshop für Photogrammetrische & Bildverarbeitungs-Techniken bei Videoüberwachung, Biometrie und Biomedizin in Moskau. Die Genauigkeit von Bewegungssoftware variiert demnach zwischen 79 und 84%, was schon als Fortschritt gefeiert wird. Eine Gesichtserkennung durch Bewegtbildkameras ist in jedem sechsten Fall fehlerhaft.

Caspar meint: „Ein exakter Abgleich der Daten kann nicht erreicht werden. Die biometrischen Merkmale werden nicht auf Gleichheit, sondern nur auf hinreichende Ähnlichkeit getestet.“ Beim Bezahlen wäre dies ein heikles Spiel mit Wahrscheinlichkeiten und Unwägbarkeiten. Jörg Schreiner, Softwareexperte und Managing Partner des Unternehmensberaters co-shift, geht davon aus, dass WeChat Verhaltensprofile der KundInnen nutzt, um Irrtümer bei der Gesichtserkennung zu vermeiden: „Darüber könnte ich jederzeit feststellen, ob die Person, die eine Identität vorgibt, auch tatsächlich diese Person ist.“ Ein solches Vorgehen ist für DatenschützerInnen erst recht nicht akzeptabel. Marit Hansen, Datenschutzbeauftragte des Landes Schleswig-Holstein, befürchtet, dass WeChat zur Beweissicherung einer Bezahlung Gesichtsfotos speichert – samt Zeit und Ort des Kaufs. Dadurch könnten detaillierte Bewegungsprofile von KundInnen gezeichnet werden, die wiederum Potenzial für Marketing hätten. Mirko Hüllemann, Gründer und Geschäftsführer der Paymentfirma Heidelpay, ergänzt: „Als Omni-Channel gäbe es für WeChat unendlich viele Möglichkeiten, entsprechende Botschaften über seinen Messenger auszusenden.“

In Europa gibt es strengere Bestimmungen als in China. Und doch rechnet Datenschützerin Hansen damit, dass Bezahlsysteme via Gesichtserkennung in absehbarer Zeit auch für Firmen wie Facebook oder Amazon ein Thema werden: „Wir sind auf dem Weg zu Welt-Datenbanken mit allen Gesichtern von allen Menschen.“ Die Datenschutz-Grundverordnung (DSGVO) schließt einen solchen Service auch in Europa nicht generell aus. Artikel 9 erlaubt Konzernen wie Facebook, biometrische Daten wie Gesichtsbilder zu verarbeiten, wenn Nutzende in die Verarbeitung zu einem bestimmten Zweck eingewilligt haben. Laut Artikel 7 DSGVO müssen sie dafür exakt informiert werden, was mit ihren biometrischen Daten geschieht und welche Konsequenzen deren Verwendung hat. Aus Sicht von Marit Hansen genügt Facebook diesen Vorgaben nicht: „Im Augenblick genügen Facebooks Informationen nicht, um zu sagen: Das ist datenschutzkonform. Ich sehe die Gefahr, dass ein solches System auch bei Facebook eingeführt wird – selbst wenn es nicht völlig im Einklang mit den europäischen Datenschutzbestimmungen stünde. Es gibt viele Leute, die dabei mitmachen.“

Solange KundInnen einen Mehrwert in einer neuer Technologie sehen, ist es schwer, diese aus Gründen des Datenschutzes aufzuhalten. Und das Potenzial bei Facebook als weltweit größtem Sozialen Netzwerk wäre nochmal höher als bei WeChat. Zusammen mit den hauseigenen Produkten WhatsApp und Instagram kontrolliert Facebook nahezu den gesamten Messenger-Markt der

westlichen Welt. Täglich nutzen mehr als zwei Milliarden Menschen die Dienste. Wer sieht, was Facebook tut, um die drei Angebote zu verknüpfen, kann erahnen, in welch großem Stil Facebook ein Bezahlsystem per Gesichtserkennung ausrollen könnte. Payment-Experte Hüllemann hält es für vorstellbar, dass eine auf Facebook gespeicherte Gesichtserkennung für eine Zahlung per WhatsApp ausgedehnt werden könnte: „Wenn ich bei WhatsApp zielgerichtete Werbung geschickt bekomme und über dieselbe Funktion im Laden auch noch bezahlen kann, ist das doch eine große Erleichterung für die Menschen" (Bohnensteffen, Bezahlen per Gesicht: WeChat prescht in China vor — doch die Schöne Neue Welt des Einkaufens alarmiert Datenschützer, www.businessinsider.de 20.09.2019).

Ecuador

Datenleck betrifft fast alle BürgerInnen

Am 16.09.2019 haben Sicherheitsforscher öffentlich gemacht, dass durch eine unsachgemäß konfigurierte Datenbank zahlreiche vertrauliche persönliche Daten von nahezu allen EinwohnerInnen Ecuadors frei im Internet zugänglich waren – darunter viele Kinder, aber auch der Präsident des Landes oder der Wikileaks-Gründer Julian Assange. Auf einem Elasticsearch-Server waren demnach rund 20,8 Millionen Datensätze online abrufbar – ein Passwort habe es nicht gegeben. Die Datensätze enthüllen persönliche Informationen der EinwohnerInnen samt Familienverhältnissen und Verwandtschaftsbeziehungen, Einwohnermeldedaten, Finanzdaten, Informationen zum Arbeitsplatz sowie zu angemeldeten Fahrzeugen.

Im Zuge der Ermittlungen zu dem Daten-Leak hat die zuständige Staatsanwaltschaft zwei Vertreter des offenbar verantwortlichen Unternehmens Novaestrat vor Ort vorübergehend festgenommen. Außerdem wurden die Geschäftsräume und eine Wohnung durchsucht. Insgesamt seien fünf Computer, sowie weitere Geräte und Dokumente beschlagnahmt worden. Außerdem hätten die Ermittler mitgeteilt, dass sie davon ausgehen, dass die Daten von mindestens sechs öffentlichen Einrichtungen gestohlen oder auf illegalen Wegen erworben worden seien. Vertreter des Ministeriums für Telekommunikation und Informationssicherheit teilten mit, dass Novaestrat nicht im Besitz der Daten hätte sein dürfen. Gleichzeitig sei aber versichert worden, dass das Unternehmen keine vom Staat betriebenen Server gehackt habe. Es bestehe der Verdacht, dass Novaestrat unter der vorigen Regierung an die Daten gelangt sei, als es mehrere Regierungsaufträge erhalten habe. In dem südamerikanischen Land soll nun ein neues Datenschutzgesetz vorangetrieben werden (Holland, Riesiges Datenleck in Ecuador: Erste Festnahmen und neue Details, www.heise.de 18.09.2019, Kurzlink: https://heise.de/-4533124).

Technik-Nachrichten

Genetische Altersbestimmung

Anhand von sog. epigenetischer Markierungen im Erbgut können Fraunhofer-Forschende auf das biologische Alter einer Zellprobe schließen. Ebenso wie der Mensch als Ganzes altert auch sein Erbgut. Ein Alterungsmechanismus ist die Methylierung, bei der kleine Moleküle, sogenannte Methylgruppen, an die DNA angeheftet werden. Oftmals haben diese Methylierungen eine regulatorische Funktion und sind reversibel. Doch unter dem Strich nimmt das Ausmaß der Methylierung im Verlauf des Lebens zu. Fraunhofer-Forscher haben im Projekt „DrugTarget" eine Methode entwickelt, um anhand der Methylierungen das Alter eines Menschen zu bestimmen. Ein Mundschleimhautabstrich und dessen genetische Analyse einschließlich des Methylierungszustands bilden die Grundlage des Alterungstests. Eine vom Fraunhofer-Institut für Molekularbiologie und Angewandte Ökologie (IME) entwickelte Software wertet die Methylierungen aus und errechnet daraus das biologische Alter der Testperson. Bei Versuchen mit 150 ProbandInnen lag das Programm maximal ein paar Monate neben dem chronologischen Alter. Die Firma Cerascreen bietet den Test bereits als Life-Style-Produkt gesundheitsbewussten Personen an, die wissen wollen, wie biologisch jung ihr Körper tatsächlich ist.

Die Fraunhofer-Forschung verfolgt ein anderes Ziel. Methylierungen blockieren die Aktivität des jeweiligen Gens und können zur Entstehung von Krankheiten beitragen. Die Wissenschaftler möchten deswegen gezielt Methylierungen einzelner Gene aufheben. Fraunhofer-Forscher Carsten Claussen erläutert: „Heute gibt es riesige Datenbanken mit mehreren Tausend Wirkstoffen, die wir im Labor durchtesten wollen, um herauszufinden, ob diese bei bestimmten Methylierungen wirken." Zusätzlich will das Team neue Wirkstoffe entwickeln und testen.

Wesentlichen Anteil daran soll die eigens entwickelte Software haben: „Der Algorithmus ist in der Lage, auch bislang unbekannte Felder im Erbgut zu finden, in denen relevante Gene stecken", erklärt Claussen und denkt dabei vor allem an Gene, die aufgrund ihrer Methylierung ausfallen und so zum Ziel für Therapien werden könnten. Die Anwendung erleichtern soll ein Programm, welches das Fraunhofer-Institut für Angewandte Informationstechnik (FIT) beisteuert, so Carina Goretzky vom FIT: „Damit wird es möglich, die genetische Information beispielsweise mit der Suche in internationalen Datenbanken und öffentlichen Listen zu verknüpfen – etwa, wenn in den Daten plötzlich ein auffälliges Gen angezeigt wird. So kann man schnell nachprüfen, ob das Gen schon bekannt ist, oder ob bereits bestimmte Wirkstoffe existieren, die interessant sein könnten" (Mit DNA-Test das biologische Alter bestimmen, biooekonomie.de 15.08.2019).

Rechtsprechung

EuGH

Opt-out genügt nicht beim Cookie-Setzen

Der Europäische Gerichtshof (EuGH) in Luxemburg hat mit Urteil vom 01.10.2019 entschieden, dass das Setzen von Werbecookies ein explizites Opt-in der Nutzenden voraussetzt (C-673/17). Gemäß einer Vorlage durch den deutschen Bundesgerichtshof (BGH) in einem Rechtsstreit zwischen dem Verbraucherzentrale Bundesverband (vzbv) und der Gewinnspielfirma Planet49 entschied der EuGH, dass Webseitenbetreiber die Nutzenden deutlich ausführlicher über die Sammlung von Nutzerdaten und die Verwendung von Cookies informieren müssen, als sie das heute vielfach tun. Einer geplanten Cookie-Nutzung müssen die Nutzenden explizit zustimmen. Es genügt nicht, dass sie einfach bestätigen, dass sie die bereitgestellten Cookie-Informationen gelesen und verstanden hätten. Sie müssen ausführlich über Zweck, Dauer und etwaige Weitergabe von Daten informiert werden.

Im vorliegenden Fall hatte die Gewinnspielfirma die Häkchen zur Zustimmung der Nutzer zur Cookie-Verwendung bereits vorab ausgefüllt. Die Nutzenden mussten nur noch auf „Ok" klicken. Eine solche implizite Zustimmung (Opt-out) genügt gemäß Art. 5 Abs. 3 der europäischen Telekommunikations-Datenschutz-Richtlinie (Cookie-Richtlinie) nicht. Die danach notwendige aktive Zustimmung setzt voraus, dass die Nutzenden das Häkchen selbst setzen (Opt-in). Vor allem in Deutschland ist das unüblich, obgleich die Cookie-Richtlinie diese explizite Zustimmung bereits seit 2009 fordert. Der mit der Cookie-Richtlinie angestrebte Schutz wird dahingehend beschrieben, dass damit alle in „Endgeräten gespeicherten Informationen" erfasst sein sollen, auch „‚Hidden Identifiers' oder ähnliche Instrumente, die ohne das Wissen der Nutzer in deren Endgeräte eindringen" (Rn. 70).

Grundsätzlich sind Mitgliedsstaaten dazu verpflichtet, solche EU-Richtlinien innerhalb von zwei Jahren in nationales Recht zu überführen. Deutschland war aber der Auffassung, dass die Cookie-Informationspflichten durch das Telemediengesetz von 2007 (TMG) bereits mit EU-Recht konform umgesetzt seien. Gemäß § 15 Abs. 3 TMG genügt es, dass den Nutzenden eine Widerspruchslösung angeboten wird. Das Urteil kann als Ansage an den deutschen Gesetzgeber gewertet werden, das deutsche Recht an die EU-Regeln anzupassen. Diese Aufgabe könnte allerdings auch der BGH übernehmen, indem dieser angesichts der klaren Worte aus Luxemburg das TMG in diesem Punkt für nicht anwendbar erklärt oder festlegt, dass das TMG so auszulegen ist, wie es der EuGH nun vorgeschrieben hat. Der vzbv begrüßte das Urteil, weil es die digitale Privatsphäre stärke.

Das Luxemburger Urteil ist nicht überraschend. Die Nichtumsetzung der Cookie-Richtlinie wird von DatenschützerInnen seit langem kritisiert. Die deutsche Datenschutzkonferenz (DSK) hat darüber hinausgehend die Position eingenommen, dass das TMG insgesamt nicht mehr anwendbar sei. Für Webseitenbetreiber gelte nur noch die Datenschutz-Grundverordnung (DSGVO). Bußgelder der Datenschutzaufsichtsbehörden liegen nun zumindest im Bereich des Möglichen. Viele IT-Anwälte empfehlen deshalb eigentlich schon länger eine mit EU-Recht konforme Einwilligungspraxis (Muth, Gericht verlangt mehr Klicks, SZ 02./03.10.2019, 23).

EuGH

Kein weltweites „Recht auf Vergessenwerden"

Mit Urteil vom 24.09.2019 hat der Europäische Gerichtshof (EuGH) in Luxemburg entschieden, dass der Betreiber einer Suchmaschine nicht verpflichtet ist, eine Auslistung in allen Versionen seiner global verfügbaren Suchmaschine vorzunehmen (C-507/17). Diese Pflicht bezieht sich auf die mitgliedstaatlichen Versionen. Zudem muss er Maßnahmen ergreifen, um die Internetnutzenden davon abzuhalten, von einem Mitgliedstaat aus auf die entsprechenden Links in Nicht-EU-Versionen der Suchmaschine zuzugreifen.

Mit Beschluss vom 10.03.2016 hatte die französische Datenschutzaufsichtsbehörde, die Commission nationale de l'informatique et des libertés (CNIL, Nationaler Ausschuss für Informatik und Freiheitsrechte, Frankreich) gegen die Google Inc. eine Sanktion von 100.000 Euro verhängt. Google hatte sich geweigert, in den Fällen, in denen ein Auslistungsantrag erfolgreich ist, die Auslistung auf sämtliche Domains seiner Suchmaschine anzuwenden. Das Unternehmen war zuvor von der CNIL am 21.05.2015 aufgefordert worden, die Auslistung auf alle Domains zu erstrecken, kam dieser Aufforderung aber nicht nach. Es entfernte die betreffenden Links nur aus den Ergebnissen, die bei Sucheingaben auf Domains angezeigt wurden, die den Versionen ihrer Suchmaschine in den Mitgliedstaaten entsprachen, und erhob beim Conseil d'État (französischer Staatsrat, das höchste Gericht des Landes) Klage auf Nichtigerklärung des Beschlusses vom 10.03.2016. Google vertrat die Ansicht, das Auslistungsrecht setze nicht zwangsläufig voraus, dass streitige Links ohne geografische Beschränkung auf sämtlichen Domains seiner Suchmaschine entfernt werden müssten. Der Conseil d'État legte dem EuGH Fragen zur Vorabentscheidung vor.

In seinem Urteil wies der EuGH auf sein früheres Urteil zum „Recht auf Vergessenwerden" vom 13.05.2014 hin (C-131/14). Danach kann ein Suchmaschinenbetreiber, es handelte sich auch um Google, verpflichtet werden, von der Ergebnisliste, die nach einer Namenssuche angezeigt wird, Links zu von Dritten veröffentlichten Websites mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Websites nicht vorher

oder gleichzeitig gelöscht werden und sogar auch dann, wenn ihre Veröffentlichung auf den Websites als solche rechtmäßig ist.

Der EuGH bestätigte nun, dass das europäische Datenschutzrecht anwendbar ist, da Google im französischen Hoheitsgebiet eine Niederlassung besitzt und Tätigkeiten ausübt, insbesondere gewerbliche und Werbetätigkeiten, die untrennbar mit der Verarbeitung personenbezogener Daten zum Betrieb der betreffenden Suchmaschine verbunden sind. Die Suchmaschine führt unter Berücksichtigung der Verbindungen zwischen ihren verschiedenen nationalen Versionen im Rahmen der Tätigkeiten der französischen Niederlassung der Google Inc. eine einheitliche Verarbeitung personenbezogener Daten aus. Das Gericht bestätigte, dass in einer globalisierten Welt der Zugriff von Internetnutzenden, insbesondere solcher, die sich außerhalb der Union befinden, auf die Listung eines Links, der zu Informationen über eine Person führt, deren Interessenschwerpunkt in der Union liegt, auch innerhalb der Union unmittelbare und erhebliche Auswirkungen auf diese Person haben kann. Nur mit einer weltweiten Auslistung könne somit das Schutzziel des Unionsrechts vollständig erreicht werden. Zahlreiche Drittstaaten kennen kein solches Auslistungsrecht. Zudem sei das Recht auf Schutz personenbezogener Daten kein uneingeschränktes Recht. Es müsse im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten müsse mit der Informationsfreiheit der Internetnutzenden abgewogen werden, wobei diese Abwägung weltweit unterschiedlich ausfallen könne. Der Unionsgesetzgeber habe eine solche Abwägung in Bezug auf die Reichweite einer Auslistung nicht über die Union hinaus durchgeführt. Einem Wirtschaftsteilnehmer wie Google sollte nicht eine Pflicht zur Auslistung für die nicht mitgliedstaatlichen nationalen Versionen seiner Suchmaschine auferlegt werden. Das Unionsrecht enthalte keine Instrumente und Kooperationsmechanismen im Hinblick auf die Reichweite einer Auslistung über die Union hinaus.

Nach derzeitigem Stand sei ein Suchmaschinenbetreiber, der einem Auslistungsantrag der betroffenen Person – gegebenenfalls auf Anordnung einer Aufsichts- oder Justizbehörde eines Mitgliedstaats – stattgibt, nach Unionsrecht nicht verpflichtet, eine solche Auslistung in allen Versionen seiner Suchmaschine vorzunehmen. Die Pflicht bezieht sich auf alle mitgliedstaatlichen Versionen der Suchmaschine. Dabei sind hinreichend wirksame Maßnahmen zu ergreifen, um einen wirkungsvollen Schutz der Grundrechte der betroffenen Person sicherzustellen. Eine solche Auslistung muss daher erforderlichenfalls von Maßnahmen begleitet sein, die es tatsächlich erlauben, die Internetnutzenden, die von einem Mitgliedstaat aus eine Suche anhand des Namens der betroffenen Person durchführen, daran zu hindern oder zumindest zuverlässig davon abzuhalten, über die im Anschluss an diese Suche angezeigte Ergebnisliste mittels einer Nicht-EU-Version der Suchmaschine auf die Links zuzugreifen, die Gegenstand des Auslistungsantrags sind (Geoblocking). Schließlich stellte der EuGH fest, dass nach derzeitigem Stand das Unionsrecht zwar keine Auslistung in allen Versionen einer Suchmaschine vorschreibt, doch verbietet es dies auch nicht. Daher blieben die Behörden eines Mitgliedstaats befugt, anhand von nationalen Schutzstandards für die Grundrechte eine Abwägung zwischen dem Recht der betroffenen Person auf Achtung des Privatlebens und auf Schutz der sie betreffenden personenbezogenen Daten einerseits und dem Recht auf freie Information andererseits vorzunehmen und nach erfolgter Abwägung gegebenenfalls dem Suchmaschinenbetreiber aufzugeben, eine Auslistung in allen Versionen seiner Suchmaschine vorzunehmen (Gerichtshof der Europäischen Union, PM Nr. 112/19 v. 24.09.2019).

EuGH

Verpflichtung zur Löschung von Hassrede ist nachhaltig und global möglich

Gemäß einem Urteil des Europäischen Gerichtshofs (EuGH) vom 03.10.2019 können Online-Dienste wie Facebook gezwungen werden bei einer rechtswidrigen Beleidigung nach weiteren wortgleichen oder ähnlichen Äußerungen zu suchen und diese zu löschen (C-18/18). Hässliche Posts und Tweets und Comments waren bisher nur begrenzt gerichtlich in den Griff zu bekommen. Mit dem Urteil des EuGH soll der Rechtsschutz zumindest ein wenig verbessert werden, indem Plattformen wie Facebook verpflichtet werden, bei der Tilgung rechtswidriger Inhalte effektiver vorzugehen. Sie können nicht nur verpflichtet werden, exakt den einen gerichtlich beanstandeten Post zu löschen, sondern auch sämtliche wort- und sinngleichen Inhalte. Der EuGH eröffnet zudem den Gerichten einen Weg, um Onlinedienste zur weltweiten Löschung zu verdonnern.

Auslöser des Verfahrens war eine Klage der österreichischen Politikerin und ehemaligen Grünen-Vorsitzenden Eva Glawischnig. Sie hatte sich 2016 in der Einwanderungspolitik zu Wort gemeldet, und zwar mit der damals eher unpopulären Forderung, die Mindestsicherung für Flüchtlinge beizubehalten. Es folgte die erwartbare Beschimpfung auf Facebook. Von einem Account unter falschem Namen aus wurde sie als „miese Volksverräterin“ und „korrupter Trampel“ beschimpft, und als jemand, die in ihrem Leben noch keinen Cent mit ehrlicher Arbeit verdient habe. Und überhaupt, die Grünen seien eine „Faschistenpartei“.

Facebook löschte die Posts auf gerichtliche Anordnung hin nur zögerlich und zudem begrenzt auf Österreich; Glawischnig klagte. Der Oberste Gerichtshof Österreichs rief daraufhin den EuGH an mit der Frage: Wie aktiv, wie wirkungsvoll, wie nachhaltig muss ein Onlinedienst gegen die Verbreitung solcher Beleidigungen auf der eigenen Plattform vorgehen? Der EuGH stellte nun klar, dass die Gerichte der Mitgliedsstaaten den Diensten ein forsches Vorgehen gegen die Multiplizierung der Hassposts zumuten dürfen. Diese können zunächst zur Löschung und Sperrung wortgleicher Inhalte verpflichtet werden. Facebook muss von sich aus nach den Wortgruppen „Glawischnig“, „miese Volksverräterin“ und „korrupter Trampel“ suchen und löschen. Gleiches gilt für sinngleiche Inhalte, wobei der

EuGH hier eine Einschränkung macht. Diese Verpflichtung gilt nur für minimale Variationen des verbotenen Posts, also für derart geringfügige Abweichungen, dass sie sich noch mit den Mitteln der Technik aufspüren lassen. Der EuGH will vom Bauprinzip der Richtlinie über den elektronischen Rechtsverkehr nicht abweichen, wonach sogenannte Hosting-Anbieter wie Facebook nicht verpflichtet sind, ihre Dienste ständig nach rechtswidrigen Inhalten zu scannen. Löschen müssen sie erst, wenn sie über beleidigende Nachrichten informiert werden: „notice and take down". „Take down" soll wirklich „take down" bedeuten.

Der EuGH spielt damit den Ball wieder zurück an die Gerichte der EU-Staaten, die per Gesetz entscheiden müssen, wie stark sie die Onlinedienste in die Pflicht nehmen. Gemäß dem Würzburger Anwalt Chan-jo Jun besteht insofern für Deutschland noch Luft nach oben: „Bisher hatte die deutsche Rechtsprechung angenommen, dass es weder eine Verpflichtung gebe, gleichartige Inhalte überall zu löschen, noch die Verpflichtung, den Upload entsprechender Inhalte zu verhindern." Er weist darauf hin, dass bei der Verletzung von Urheberrechten inzwischen die plattformübergreifende Entfernung von Musiktiteln verlangt werde. Der bayerische Justizminister Georg Eisenreich (CSU) schlug vor, das zwei Jahre alte Netzwerkdurchsetzungsgesetz entsprechend zu erweitern. Wenn Betroffene gegen jeden einzelnen Post Beschwerde einlegen müssten, seien diese „praktisch wehrlos".

Bei der Frage, ob Onlinedienste eine Löschung auf das Gebiet des jeweiligen Landes beschränken dürfen, so wie dies mit dem sogenannten Geoblocking geschieht, sind gemäß dem Urteil nun die nationalen Gerichte am Zug. Aus EU-Sicht jedenfalls sind sie durch das Völkerrecht nicht an der Anordnung weltweiter Löschpflichten gehindert. Rechtsanwalt Jun meinte, dass Geoblocking keinen effektiven Rechtsschutz liefere, weil solche Blockaden umgangen werden könnten.

Der EuGH zeigt damit der Justiz und dem Gesetzgeber die Instrumente, mit denen sie soziale Medien in die Pflicht nehmen können. Die Standards für Beleidigung aber legen nationale Gerichte selbst fest. Von ihren Entscheidungen hängt ab, ob Betroffene wirksam gegen Hass und Hetze geschützt werden. In diesem Zusammenhang sorgte kurz vor dem EuGH-Urteil ein Beschluss des Landgerichts Berlin für große Empörung in der Öffentlichkeit, wonach sich die Grünen-Politikerin Renate Künast Beschimpfungen als „Stück Scheiße" und „Geisteskranke" gefallen lassen müsse. Künast hat nun, unterstützt von der Initiative Hate-Aid, Beschwerde eingelegt, ein Schritt, um die Standards klarer zu definieren: „Im Unterschied zum Landgericht halte ich die getätigten Äußerungen über mich keineswegs für hinnehmbar! Als demokratische Gesellschaft dürfen wir einen solchen Umgangston nicht akzeptieren" (Janisch, Facebooks lange Leine wird ein bisschen kürzer, www.sueddeutsche.de 03.10.2019 = Janisch, Löschen ist Pflicht, SZ 04.10.2019, 1, 4, 7).

BVerwG

Datenschutzbehörde darf Facebook-Fanpagebetrieb untersagen

Das Bundesverwaltungsgericht (BVerwG) in Leipzig hat mit Urteil vom 11.09.2019 entschieden, dass ein Betreiber eines im sozialen Netzwerk Facebook unterhaltenen Unternehmensauftritts (Fanpage) verpflichtet werden kann, seine Fanpage abzuschalten, falls die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist (BVerwG 6 C 15.18).

Im Jahr 2011 hatte die schleswig-holsteinische Datenschutzaufsicht, das Unabhängige Landeszentrum für Datenschutz (ULD), die Wirtschaftsakademie Schleswig-Holstein, eine in Kiel ansässige Bildungseinrichtung der Industrie- und Handelskammern des Landes (IHK), verpflichtet, unter der Geltung der Datenschutzrichtlinie (Richtlinie 95/46/EG), die von ihr bei Facebook betriebene Fanpage zu deaktivieren. Der Bescheid beanstandete, dass Facebook bei Aufruf der Fanpage auf personenbezogene Daten der Internetnutzenden zugreift, ohne dass diese gemäß den Bestimmungen des Telemediengesetzes (TMG) über Art, Umfang und Zwecke der Erhebung sowie ein Widerspruchsrecht gegen die Erstellung eines Nutzungsprofils für Zwecke der Werbung oder Marktforschung unterrichtet würden. Ein gegenüber der Klägerin als Betreiberin der Fanpage erklärter Widerspruch des Nutzers bleibe mangels entsprechender technischer Einwirkungsmöglichkeiten folgenlos.

Die Klage hatte in den Vorinstanzen Erfolg gehabt. Das Oberverwaltungsgericht Schleswig-Holstein (OVG) hatte eine datenschutzrechtliche Verantwortlichkeit der Klägerin abgelehnt, weil sie keinen Zugriff auf die erhobenen Daten habe (DANA 4/2014, 184 f.). Im Revisionsverfahren wandte sich das ULD an das BVerwG, das mit Beschluss vom 25.02.2016 eine Vorlage beim Europäischen Gerichtshof (EuGH) vornahm (BVerwG 1 C 28.14, DANA 2/2016, 107). Mit Urteil vom 05.06.2018 entschied der EuGH, dass der Betreiber einer Fanpage für die durch Facebook erfolgende Datenverarbeitung mitverantwortlich ist, da er durch den Betrieb der Fanpage Facebook den Zugriff auf die Daten der Fanpage-Besuchenden ermöglicht (C-210/16, ausführlich dazu Weichert, DANA 1/2019, 4 ff.).

Das BVerwG hat auf der Grundlage dieser bindenden Vorgabe das Berufungsurteil aufgehoben und den Rechtsstreit an das OVG zurückverwiesen. Um das von der Datenschutzrichtlinie bezweckte hohe Datenschutzniveau möglichst zügig und wirkungsvoll durchzusetzen, konnte sich das ULD bei der Auswahl unter mehreren datenschutzrechtlichen Verantwortlichen vom Gedanken der Effektivität leiten lassen und ermessenfehlerfrei die Klägerin für die Herstellung datenschutzkonformer Zustände bei Nutzung ihrer Fanpage in die Pflicht nehmen. Es musste nicht gegen eine der Untergliederungen oder Niederlassungen von Facebook vorgehen, weil das wegen der fehlenden Kooperationsbereitschaft von Facebook mit erheblichen tatsächlichen und rechtlichen Unsicherheiten verbunden gewesen wäre. Erweisen sich die bei Aufruf der Fanpage ablaufenden Datenverarbeitungen als rechtswidrig, so stellt die Deaktivierungsanordnung ein verhältnismäßiges Mittel dar, weil der Klägerin keine anderweitige Möglichkeit zur Herstellung

datenschutzkonformer Zustände offensteht.

Um die Rechtswidrigkeit der beanstandeten Datenverarbeitungsvorgänge festzustellen, bedarf es einer näheren Aufklärung der tatsächlichen Umstände durch das OVG. Die Rechtmäßigkeit der bei Aufruf der klägerischen Fanpage ablaufenden Datenverarbeitungsvorgänge ist dabei an den Vorgaben des im Zeitpunkt der letzten Behördenentscheidung gültigen Datenschutzrechts, insbesondere an den Vorschriften des Telemediengesetzes zu messen (BVerwG, PE Nr. 62/2019 v. 11.09.2019, Datenschutzbehörde kann Betrieb einer Facebook-Fanpage untersagen).

BVerwG

EuGH-Vorlage wegen deutscher Vorratsdatenspeicherung

Das Bundesverwaltungsgericht (BVerwG) in Leipzig hat mit Beschluss vom 25.09.2019 dem Europäischen Gerichtshof (EuGH) im Luxemburg die Frage vorgelegt, ob die deutsche Vorratsspeicherung von Telekommunikationsdaten mit dem Europarecht vereinbar ist (6 C 12.18 u. a). Die Vorratsdatenspeicherung erlaubt es Strafverfolgungsbehörden, auf Internet- und Telefondaten zuzugreifen, die private Telekommunikationsanbieter zu diesem Zweck auf Vorrat bereithalten müssen. Geklagt hatten dagegen zwei solche Dienstleister. Sie wenden sich gegen die ihnen durch § 113a Abs. 1 i. V. m. § 113b Telekommunikationsgesetz (TKG) auferlegte Speicherpflicht. Gemäß dem im Jahr 2015 beschlossenen Gesetz zur „Mindestspeicherpflicht und Höchstspeicherdauer von Verkehrsdaten" hätte die Pflicht zur Vorratsdatenspeicherung vom 01.07.2017 an bestanden. Doch liegen die Regelungen derzeit auf Eis. Am 21.12.2016 hatte der EuGH in Bezug auf Regelungen in Schweden und Großbritannien geurteilt, dass eine allgemeine und anlasslose Speicherung von Daten unzulässig ist. Ihr stehe die Telekommunikations-Datenschutzrichtlinie und die EU-Grundrechtecharta entgegen. Ausnahmen wurden den Mitgliedstaaten nur zur Bekämpfung schwerer Straftaten erlaubt. Schon die Speicherung sei auf das unbedingt Notwendige zu begrenzen, der Zugang der Sicherheitsbehörden in den Ausnahmefällen von einer gerichtlichen Kontrolle abhängig zu machen (C-203/15, C-698/15, DANA 2017, 60 f.).

Daraufhin stellte das Oberverwaltungsgericht Nordrhein-Westfalen die Speicherpflicht mit Beschluss vom 22.06.2017 in Bezug auf den Internetprovider SpaceNet AG in Frage (13 B 238/17, DANA 2017, 177 f.). Im Anschluss an diese Entscheidung setzte die zuständige Bundesnetzagentur die Pflicht für Telekommunikationsanbieter generell aus. Das Verwaltungsgericht (VG) Köln befreite daraufhin die Deutsche Telekom mit Urteil vom 20.04.2018 von der Speicherpflicht (9 K 741/17) und ließ wegen grundsätzlicher Bedeutung die Sprungrevision zum BVerwG zu.

Das BVerwG möchte nun vor allem klären, ob die deutschen Regelungen den britischen und schwedischen so ähnlich sind, dass sich die Aussagen des EuGH übertragen lassen. Daran haben die Leipziger Richter offenbar Zweifel. So ist der Kreis der von der Speicherpflicht erfassten Kommunikationsmittel und die Speicherdauer gegenüber den schwedischen und britischen Regelungen in der deutschen Variante reduziert. Nach deutschem Recht werden nur Verbindungsdaten, nicht aber Daten über aufgerufene Internetseiten gespeichert. Ferner enthalten die deutschen Regelungen strengere Beschränkungen für den Schutz der gespeicherten Daten.

Angesichts des mit den neuen Telekommunikationsmitteln verbundenen spezifischen Gefahrenpotenzials bestehe ein Spannungsverhältnis zwischen den in den Art. 7 und 8 Grundrechtecharta verankerten Grundrechten auf Achtung der Privatsphäre sowie auf Schutz personenbezogener Daten einerseits und der aus Art. 6 der Charta folgenden Pflicht der Mitgliedstaaten andererseits, die Sicherheit ihrer Bürger zu gewährleisten. Ein ausnahmsloses Verbot der anlasslosen Vorratsdatenspeicherung würde den nationalen Gesetzgeber auf dem Gebiet der Strafverfolgung und der Gewährleistung der öffentlichen Sicherheit – was zu den Kernkompetenzen der Nationalstaaten gehört – erheblich einschränken.

Dieses Argument hatte auch die britische Regierung für ihre Geheimdienste in einem weiteren Vorratsdatenspeicher-Verfahren vor dem EuGH Anfang September 2019 vorgebracht. Sie meinte, dass sich auch aus der neueren Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) zu Art. 8 der Menschenrechtskonvention Anhaltspunkte ergeben, die pro Sicherheitskompetenzen der Nationalstaaten streiten. Das BVerwG bezweifelte nun in seinem Beschluss, dass die Grundsatzentscheidung des EuGH 2016 als ein generelles Verbot der anlasslosen Vorratsdatenspeicherung in Europa verstanden werden muss. Möglicherweise komme es für Ausnahmen auch auf die Erheblichkeit der zu bekämpfenden Gefahren an sowie auf eine angemessene „Kompensation" durch restriktiven Zugriff und hohe Sicherheitsanforderungen. Die Wiedereinführung der Vorratsdatenspeicherung könnte also allein von ihrer Ausgestaltung abhängen.

Sicherheitspolitiker und Polizeibehörden fordern immer wieder die Speicherung von Verbindungsdaten, um etwa Terroranschläge verhindern oder Kinderpornografie bekämpfen zu können. KritikerInnen halten die massiven Grundrechtseingriffe dagegen für illegal und bezweifeln den Nutzen. Oliver Süme, Vorstand des Verbandes der deutschen Internetwirtschaft (eco), meinte: „Wir sind überzeugt, dass wir damit nicht ein Mehr an Sicherheit erreichen würden." Es gebe mildere Mittel – etwa in konkreten Verdachtsfällen die Daten sichern zu lassen. Der stellvertretende FDP-Fraktionsvorsitzende Stephan Thomae hofft: „Jetzt wird endlich der Europäische Gerichtshof Klarheit schaffen und über die Zulässigkeit der Vorratsdatenspeicherung in Deutschland abschließend entscheiden." Schon die bisherige EuGH-Rechtsprechung hätte die Bundesregierung seines Erachtens veranlassen müssen, Alternativen zu suchen. „Denkbar wäre eine anlassbezogene, begrenzte Speicherung von Telekommunikationsdaten zur Aufklärung von Straftaten oder Abwehr konkreter Gefahren, das sogenannte Quick-Freeze-Verfahren."

Auch beim Bundesverfassungsgericht (BVerfG) liegen Beschwerden gegen die Vorratsdatenspeicherung. Es wies die Beschwerdeführer bereits Anfang 2018

darauf hin, dass es für das juristische Schicksal der Vorratsdatenspeicherung neben dem Grundgesetz als Maßstab insbesondere auf die Vorgaben aus der Rechtsprechung des EuGH ankommen dürfte. Im Entscheidungsplan des BVerfG ist die Vorratsdatenspeicherung für 2019 noch angesetzt, wobei unklar bleibt, ob das BVerfG dann eine Entscheidung in der Sache treffen wird.

Derweil suchen ungeachtet des rechtlichen Schicksals der bisherigen Modelle die Justizminister auf europäischer Ebene bereits nach einer neuen tragfähigen europäischen Regelung und haben die EU-Kommission in Brüssel beauftragt, eine Lösung zu suchen. Bis Ende 2019 soll dazu eine „umfassende Studie" vorgelegt werden. Die Idee geht dahin, statt eine pauschale Speicherpflicht vorzusehen spezifische Daten aufzulisten, deren Speicherung sich Strafverfolger von den Anbietern wünschen können. Neben den klassischen Providern könnten dann nach den Plänen auch Social-Media-Anbieter wie z.B. Facebook zur Speicherung auf Vorrat verpflichtet werden (Sehl, Alle Augen auf Luxemburg, www.lto.de 25.09.2019; Janisch, Datenspeicherung nach Luxemburg, SZ 26.09.2019, 5).

BVerwG

Polizei-Kennzeichnungspflicht ist rechtens

Das Bundesverwaltungsgericht (BVerwG) in Leipzig hat mit Urteil vom 26.09.2019 festgestellt, dass die Kennzeichnungspflicht für PolizeibeamtInnen, wie sie in mehr als der Hälfte der Bundesländer existiert, verfassungsgemäß ist (2 C 32.18 u. a.). Es billigte in einem Grundsatzurteil das Polizeigesetz des Landes Brandenburg, das den BeamtInnen seit 2013 vorschreibt, ein Schild mit ihrem Nachnamen an der Uniform zu tragen. In geschlossenen Einheiten – sogenannten Hundertschaften – gilt eine modifizierte Regelung: Es besteht die Pflicht, lediglich Nummern zu tragen, die eine spätere Identifizierung ermöglichen. Geklagt hatten ein Polizeihauptmeister und eine Polizeiobermeisterin. Sie sahen sich in ihrem Recht auf informationelle Selbstbestimmung verletzt, weil ihre Identifizierbarkeit die Gefahr erhöhe, dass sie privat ausgespäht und belästigt werden könnten. Die Gewerkschaft der Polizei (GdP) hat die Klagen unterstützt. Sie sieht in den Namens- und Nummernschildern einen Ausdruck des Misstrauens gegen die Polizei.

Das BVerwG hält die Kennzeichnung für gerechtfertigt, weil sie Bürgernähe und Transparenz der Polizeiarbeit stärke. Zudem stuft sie die Identifizierbarkeit von BeamtInnen als eine Maßnahme gegen Polizeigewalt ein. Sie gewährleiste „die leichtere Aufklärbarkeit etwaiger Straftaten oder nicht unerheblicher Dienstpflichtverletzungen von Polizeivollzugsbeamten und beugt damit solchen vor". Ein aktuelles Forschungsprojekt des Bochumer Kriminologen Tobias Singelnstein ergab, dass Polizeigewalt kaum strafrechtlich verfolgt wird. Das BVerwG sieht in der Kennzeichnung auch einen gewissen Schutz für rechtmäßig handelnde PolizistInnen, die von Ermittlungen verschont bleiben, wenn sich eine Strafanzeige gleich an die richtige Adresse richtet.

Da die Argumente überall weitgehend gleich gelagert sind, lässt sich das zu Brandenburg gefällte Urteil auf die Mehrheit der Regelungen in den anderen Bundesländern übertragen. Mit seinen Namensschildern geht Brandenburg weiter als manch andere Länder, in denen lediglich Nummern ausgegeben werden. Etwas anderes gilt möglicherweise für Schleswig-Holstein, wo die Kennzeichnungspflicht durch einen ministeriellen Erlass eingeführt wurde. Das BVerwG betonte, dass in Brandenburg eine „hinreichend bestimmte gesetzliche Grundlage" besteht. Der Gesetzgeber habe die wesentlichen Entscheidungen „nach einer parlamentarischen Debatte selbst getroffen".

Es gibt in Deutschland weiterhin Länder ohne Kennzeichnungspflicht, so Bayern, Baden-Württemberg und Nordrhein-Westfalen. Das Urteil des BVerwG bestätigt, dass ein Gesetz, nach dem PolizistInnen identifizierbar sind, gemäß dem Grundgesetz erlaubt ist, verpflichtet aber nicht dazu, ein solches Gesetz einzuführen (Janisch, Polizisten müssen Kennzeichnung tragen, SZ 27.09.2019, 1).

BVerwG

BND zu Presseauskünften über exklusive Pressetermine verpflichtet

Der Bundesnachrichtendienst (BND) darf gemäß einem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 18.09.2019 nicht länger ein Geheimnis daraus machen, wann, wo und wie oft er ausgewählte JournalistInnen zu Hintergrundgesprächen einlädt (BVerwG 6 A 7.18). Die Richter gaben in Leipzig einer Klage des rechtspolitischen Korrespondenten des Berliner Tagesspiegels, Jost Müller-Neuhof, größtenteils Recht.

Seit 2013 betreibt der BND eine Form von Öffentlichkeitsarbeit und Imagepflege: Er lädt JournalistInnen ein und unterrichtet sie über Einschätzungen des Geheimdienstes. Die Einladenden müssen sich zuvor zu Stillschweigen verpflichten. BND-Sprecher Martin Heinemann erklärte vor Gericht, die Treffen dienten dazu, die Recherchen von Medien zu ergänzen oder neue Ansätze zu liefern. Zwar verrate der Dienst, gemäß dem Vortrag des BND-Anwalts Wolfram Hertel, bei solchen Runden mit jeweils etwa 30 JournalistInnen keine Geheimnisse. Es könne jedoch zu diplomatischen Verwicklungen führen, wenn der Dienst öffentlich als Quelle der Einschätzung im Ausland bekannt werde.

Zumindest die Umstände dieser Treffen und die besprochenen Themen muss der BND gemäß dem Urteil transparent machen. Der Dienst habe kein „schutzwürdiges öffentliches Interesse", solche Daten geheimzuhalten. Die Aufgabenerfüllung des BND sei nicht in Gefahr, wenn bekannt werde, wer eingeladen wurde und an welchen Treffen auch der Präsident des BND, Bruno Kahl, teilgenommen habe. Es sei „nicht ersichtlich", wie ein Bekanntwerden der bloßen Themen, also nicht der konkreten Inhalte, die Arbeit des BND gefährden würde. Auch auf die Privatsphäre der eingeladenen Journalisten bzw. deren informationelle Selbstbestimmung könne sich der BND nicht berufen. Das öffentliche Aufklärungsinteresse im Hinblick auf die Beziehungen zwischen Nachrichtendienst und Presse wiege schwerer. Der Kläger Müller-Neuhof selbst war

vom BND nicht eingeladen worden und hatte dies auch nicht verlangt, er wollte nur die Auskünfte. Der BND erklärte, er nehme die Entscheidung des Gerichts „mit Respekt zur Kenntnis“. In einigen Punkten hat sich der BND auch durchgesetzt. So muss er weiter keine Auskunft darüber geben, ob und wie er das Bundeskanzleramt über den Putschversuch in der Türkei im Juli 2016 informierte (Steinke, Keine Geheimnisse, SZ 19.05.2019, 25).

OLG Düsseldorf

Facebook darf trotz Kartellrechtsklage weiter Daten sammeln

Das Oberlandesgericht (OLG) Düsseldorf meldete mit einem Beschluss vom 26.08.2019 im Rahmen einer „bloß summarischen“ Prüfung „ernstliche Zweifel“ an der Rechtmäßigkeit des weltweit beachteten Vorgehens des deutschen Bundeskartellamtes gegen Facebook an. Auf Antrag des Datenkonzerns setzte das Gericht vorerst die Vollziehbarkeit des kartellrechtlichen Verbots aus und sparte dabei nicht mit Kritik an den Kartellwächtern (Az. VI-Kart 1/19(V)). Im Februar 2019 hatte das Bundeskartellamt mit Blick auf Facebooks umfangreiche Datensammlung unter großem Medienecho entschieden, dass der Datenkonzern seine marktbeherrschende Stellung als Soziales Netzwerk ausnutze und NutzerInnen unfaire Konditionen auferlege. Im Kern ging es dabei um die Zusammenführung von Daten aus Facebook, Instagram, WhatsApp und anderen Quellen, etwa Webseiten, die einen Like-Button anbieten. NutzerInnen hätten keine Wahl, ob sie dem zustimmen oder nicht zustimmen. Kartellamtspräsident Andreas Mundt verordnete dem Konzern eine „innere Entflechtung“, bei der Daten aus unterschiedlichen Quellen nur noch dann zusammengeführt werden dürften, wenn NutzerInnen informiert seien und echte Entscheidungsfreiheit hatten. Mit dem Verfahren gegen Facebook wollte Mundt „kartellrechtliche Leitplanken in die Internetökonomie einziehen“.

Die Aufsichtsbehörde hatte Facebook bis zu zwölf Monate Zeit gegeben, die Maßnahmen umzusetzen. Dagegen wehrte sich der Datenkonzern vor dem OLG und kann nun einen Teilerfolg feiern: Die Frist bleibt ausgesetzt, bis das Verfahren entschieden ist. Zudem äußerte das OLG in seiner 37-seitigen Begründung „ernstliche Zweifel“ an dem gesamten Verfahren gegen Facebook. Die Entscheidung des Kartellamtes war in Politik und Medien auf breite Zustimmung gestoßen; von JuristInnen wurde aber kritisiert, hier würden Datenschutz- und Kartellrecht unzulässig vermischt. Dem schloss sich der erste Kartellsenat an: Selbst wenn die beanstandete Datenverarbeitung gegen Datenschutzbestimmungen verstoße, liege darin nicht zugleich ein Verstoß gegen das Wettbewerbsrecht. Die VerbraucherInnen würden durch die Datensammlung wirtschaftlich nicht geschwächt, denn sie würden ihre Daten bei Facebook ja nicht verlieren. Anders als bei einem klassischen Nutzungsentgelt wären Daten duplizierbar. Das Kartellamt habe auch nicht ausreichend nachgewiesen, dass Facebook aktuelle oder potenzielle Wettbewerber behindern würde.

Das OLG bezweifelt sogar, dass überhaupt Datenschutzverstöße vorliegen. Da die NutzerInnen den Nutzungsbedingungen von Facebook vor der Anmeldung zustimmen würden, könne von einem „Kontrollverlust“, wie ihn das Kartellamt festgestellt hatte, nicht die Rede sein. Die Datenverarbeitung erfolge vielmehr mit „Wissen und Wollen“ der NutzerInnen. Dass es für VerbraucherInnen sehr wohl einen Nachteil bedeuten kann, wenn Konzerne über ihre Daten verfügen und damit Verhaltensprognosen anstellen und kommerzielle Werbung schalten, wird vom OLG ebenso ignoriert wie die Tatsache, dass heute große Teile von sozialem Leben und politischer Öffentlichkeit digital vermittelt werden und dabei Facebook, Instagram und WhatsApp eine marktdominierende Position erlangt haben.

Der Direktor des Instituts für Kartellrecht an der Heinrich-Heine-Universität Düsseldorf, Rupprecht Podszun, erklärte zu dem Beschluss: „Wenn man ehrlich ist, ist das Verfahren mit der heutigen Entscheidung tot.“ Tatsächlich wird das Verfahren des Kartellamts gegen Facebook mit dem Beschluss voraussichtlich um Monate bis Jahre verzögert. Wie das Hauptsacheverfahren bei dem OLG ausgehen wird, ist nach der eindeutigen aktuellen Entscheidung absehbar. Die Hoffnung liegt nun beim Bundesgerichtshof (BGH), bei dem das Kartellamt Beschwerde einlegt. Möglicherweise wird zudem der Europäische Gerichtshof angerufen. Podszun kommentierte: „Selbst wenn das Kartellamt in einigen Jahren in letzter Instanz Recht bekommen sollte, hat sich die Situation bei den sozialen Netzwerken ja schon wieder stark weitergedreht. Dann ist eine Entscheidung von 2019, der schon dreijährige Ermittlungen vorausgegangen sind, nur noch ein historisches Kuriosum.“ Kurz vor der Entscheidung des Kartellamtes hatte Mark Zuckerberg angekündigt, man werde die unterschiedlichen Dienste seines Konzerns zusammenführen. Facebook, WhatsApp und Instagram würden für EndverbraucherInnen zwar immer noch unterschiedliche Anwendungen darstellen, aber auf einer gemeinsamen Infrastruktur laufen. Eine „innere Entflechtung“ auf Ebene der Daten, wie dem Kartellamt vorschwebt, wäre dann kaum noch möglich.

Datenschutzbehörden haben mit der Datenschutzgrundverordnung (DSGVO) zwar einige rechtliche Möglichkeiten zum Handeln, doch fehlen ihnen die Ressourcen, um den Muskelspielen der Industrie etwas entgegenzusetzen. Für die wichtige Rolle, die ihnen laut DSGVO bei der Durchsetzung des Datenschutzes zusteht, bräuchten sie mehr Geld, mehr Personal und mehr technisches Knowhow. Zudem müssen sich die Behörden bei Verfahren gegen internationale Konzerne nicht nur innereuropäisch einigen, sondern es dauert auch Jahre, bis die juristischen Auseinandersetzungen um Auslegungsfragen beigelegt sind. Den Kartellwächtern wiederum fehlen offenbar weiterhin eindeutige rechtliche Grundlagen. Dass OLG ging die vom Kartellamt vorgenommene Übertragung des wettbewerbsrechtlichen Rechtsrahmens aus dem analogen in das digitale Zeitalter nicht mit. Deshalb bleibt es auf der Tagesordnung, dass eine Expertenkommission im Auftrag der Bundesregierung Vorschläge macht, wie das Wettbewerbsrecht an die Bedingungen der digitalen Gesellschaft angepasst

werden kann (Dachwitz, Kartellamt gegen Facebook: Das OLG Düsseldorf schaut mit dem Tunnelblick auf die Datenfrage, netzpolitik.org 26.08.2019; Müller, Facbeook darf weiter sammeln, SZ 27.08.2019).

LG Dresden

Unterlassungsanspruch gegen Webseitenbetreiber wegen Google-Analytics-Einsatz

Das Landgericht (LG) Dresden hat mit Urteil vom 11.01.2019 entschieden, dass der Einsatz von Google Analytics ohne Aktivierung von anonymizeIP unzulässig ist und Unterlassungs-, Auskunfts- und Schadenersatzansprüche der betroffenen Person nach sich zieht (Az. 1a O 1582/18). Der Kläger, eine natürliche Person und einfacher Verbraucher, hat die Beklagte, die Betreiberin eines Internetportals, wegen Unterlassung, Auskunft sowie Freistellung von vorgerichtlichen Anwaltskosten in Anspruch genommen. Der Klage lag zugrunde, dass die Beklagte die personenbezogenen Daten des Klägers und insbesondere seine IP-Adresse beim Aufruf der Internetseite der Beklagten durch den Einsatz von Google Analytics (GA) ohne Zustimmung des Klägers an Server von Google in den USA übermittelt hatte, und zwar ohne sich hierbei der Funktion anonymizeIP zu bedienen. AnonymizeIP verschleiert das letzte Oktett einer IP-Adresse und soll so eine Anonymisierung gewährleisten.

Das LG hat die geltend gemachten Ansprüche des Klägers, insbesondere den Unterlassungsanspruch, mit einer Verletzung des allgemeinen Persönlichkeitsrechts (APR), also mit den §§ 823 Abs. 1 i.V.m. 1004 BGB analog begründet. Der Verweis auf das TMG, die DSGVO und das alte BDSG beschränkten sich darauf, dass keine wirksame Einwilligung erteilt worden sei und dass das Datenschutzrecht auch das APR zu schützen angetreten sei. Eine in den Allgemeinen Geschäftsbedingungen (AGB) versteckte Einwilligung akzeptierte das LG nicht, da es an „einer bewussten und eindeutigen Handlung des Nutzers“ fehlte. Das Gericht sieht in einer Übermittlung der GA-Daten an Google eine hinreichende „Schwere des Eingriffs“. Bzgl. des Auskunftsanspruchs wurde auf § 13 Abs. 8 TMG Bezug genommen. Ob durch den Einsatz von anonymizeIP tatsächlich eine Anonymisierung stattfindet, wurde vom Gericht unterstellt und nicht weiter hinterfragt.

Interessant sind auch die Ausführungen des Gerichts zu der erfolgten „Verbraucherabmahnung“. Der Kläger hatte gezielt mit technischen Mitteln nach Webseiten gesucht, auf denen Analysetools ohne Verschleierung der IP eingesetzt werden. Darin sieht das Gericht kein rechtsmissbräuchliches Verhalten i. S. v. § 242 BGB. Es sei dem Kläger mit seiner Abmahnung nicht um Geld gegangen, was dadurch zu sehen sei, dass er kostenfrei eine Mail versendet hatte, in der er eine strafbewehrte Unterlassungserklärung eingefordert hat und auch im Prozess nur die Anwaltskosten erstattet bekommen wollte. Auch interessant ist, wie das LG das Beklagtenargument zurückgewiesen hat, der Kläger hätte mit Maßnahmen des Selbstschutzes verhindern können, dass seine IP über die Webseite bei Google landet: Dies widerspräche „dem Zweck des Datenschutzrechts“: „Eine Verpflichtung dem Verletzten aufzuerlegen, sich vor einer vermuteten Rechtsverletzung selbst durch Vorkehrungen zu schützen, um eine tatsächliche Rechtsverletzung zu verhindern, widerspricht den vorgenannten Grundsätzen des Datenschutzes“. Das Urteil des LG ist rechtskräftig.

Landesgericht Feldkirch/Österreich

Immaterieller Schadenersatz wegen illegaler Speicherung über Parteiaffinitäten

Auf die Klage des Vorarlberger Anwalts Christian Wirthensohn wurde die Österreichische Post wegen der Speicherung sogenannter Parteiaffinitäten auf Schadenersatz gemäß Art. 82 Datenschutz-Grundverordnung (DSGVO) vom Landesgericht Feldkirch zur Zahlung von 800 Euro verurteilt (Gz. 57 Cg 30/19b). Mehr als ein halbes Jahr zuvor hatte die Plattform Addendum in einem Bericht aufgedeckt, dass die Post sog. Parteiaffinitäten von Millionen KundInnen berechnet und speichert. Die Kundendaten wurden mit Präferenzen zu einer möglichen Parteinähe erweitert und an wahlwerbende Parteien verkauft. Als die Datenschutzbehörde feststellte, dass die Post diese sensiblen Daten nicht hätte speichern und schon gar nicht verkaufen dürfen, kündigte das Unternehmen an, sensible Daten zur politischen Meinung aus ihren Datensätzen zu löschen. Betroffen von der Speicherung waren insgesamt rund 2,2 Millionen ÖsterreicherInnen, einer davon der klagende Anwalt.

Da die Post bestritt, dass es sich bei den Parteiaffinitäten um sogenannte sensible, also besonders zu schützende Daten handle, verklagte der Anwalt die Post im März 2019 auf immateriellen Schadenersatz über 2.500 Euro: „Wenn ich weiß, dass meine Rechte bewusst verletzt werden und damit auch noch Geld gemacht wird, dann lasse ich mir das nicht weiter gefallen.“ Anfang Juli 2019 wurde der Fall am Landesgericht Feldkirch verhandelt. Dem Betroffenen wurde Recht gegeben und vom Gericht 800 € immaterieller Schadenersatz zuerkannt.

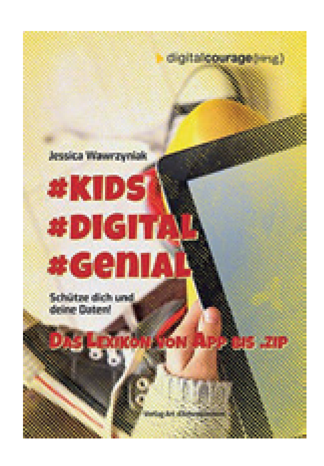
„Die Tatsache, dass die beklagte Partei [Anm.: die Post] *Parteiaffinitäten des Klägers ohne dessen Einwilligung und Information ermittelt und gespeichert hat, rechtfertigt einen immateriellen Schadenersatz. In Anbetracht der Tatsache, dass es sich einerseits bei der politischen Meinung einer Person um besonders schützenswerte und sensible Daten handelt, andererseits die von der beklagten Partei gespeicherten Parteiaffinitäten des Klägers feststellungsmäßig nicht an Dritte übermittelt wurden, erscheint ein Betrag in Höhe von EUR 800,– zur Abgeltung des vom Kläger erlittenen immateriellen Ungemachs angemessen. …*

Aus Sicht des Gerichts handelt es sich bei den von der beklagten Partei mittels Marketinganalyseverfahren ermittelten Affinitäten aufgrund der Tatsache, dass diese in weiterer Folge dem Kläger als Individuum zugeschrieben wurden, klar um sich auf eine identifizierte natürliche Person beziehende Informationen [sic], *sohin um personenbezogene Daten. …*

Auch die Frage, ob die Parteiaffinitäten unter die besonderen Kategorien personenbezogener Daten fallen, ist aus Sicht des Gerichts klar zu bejahen, da es sich um Abbildungen politischer Meinungen handelt."

Sowohl der klagende Anwalt als auch die Post haben angekündigt, gegen das Urteil Berufung einzulegen (das rechtskräftige Urteil wird dann für Anfang 2020 erwartet). Das nicht rechtskräftige Urteil könnte weitreichende Folgen haben. Betroffen waren insgesamt ca. 2,2 Millionen Personen. Der Schadenersatz würde – geht man von der Argumentation des Gerichts aus – auch allen anderen Betroffenen zustehen. Denn auch bei ihnen wurde die Parteiaffinität ohne ihr Zutun abgespeichert. Und der Schadenersatz könnte durchaus noch höher ausfallen, wenn – im Gegensatz zu diesem Fall – die sensiblen Daten auch noch – etwa an Parteien für Wahlwerbung – weiterverkauft wurden (Mayrhofer, Post-Daten: Überraschendes Urteil nach Klage auf Schadenersatz, www.addendum.org, 16.08.2019).

Buchbesprechungen



Wawrzyniak, Jessica
#Kids #Digital #Genial – Schütze dich und deine Daten
Art d' Ameublement, Bielefeld, 2018
ISBN 978-3-934636-17-0, 66 S.,
Einzelpreis versandkostenfrei 2,45 €

(tw) Das von digitalcourage herausgegebene Büchlein, das auch als Klassensatz versendet wird, wendet sich als „Das Lexikon von Apps bis .ZIP" an ältere Kinder und Jugendliche und versucht diesen das Thema Datenschutz näher zu bringen, ohne die eingesetzte Technik zu verteufeln. In einfacher Sprache werden zunächst Fragen zum Datenschutz beantwortet: Was sind private Daten, wieso sind diese Privatsache, wer sammelt diese, was steckt hinter der Datensammelei? Dann erläutert das Heftchen aus Datenschutzsicht über 100 Begriffe, gibt – nett illustriert – Tipps zum Umgang mit privaten Daten und Denkanstöße und stellt kleine Aufgaben. Damit kann in der Schule das Thema Digitalisierung und Datenschutz behandelt werden. Eine Auswahl der Begriffe: Blog, Browser, Cookie, Cloud, Cybermobbing, Darknet, FakeNews, Firewall, GPS ... Lehrkräfte erhalten mit dem Büchlein etwas in die Hand, das den Kindern einen spielerischen Zugang zum Thema ohne große Hemmschwellen ermöglicht.



Christoph J. Partsch (Hg.),
Bundesarchivgesetz, Handkommentar,
Baden-Baden 2019, Nomos Verlag

(me) Verglichen mit der Fülle an Kommentaren und Monographien, die zum Datenschutzrecht seit Inkrafttreten der DSGVO und der Novellierung des BDSG im Jahre 2018 erschienen sind, gibt es zum Bundesarchivgesetz wenig Literatur. Dieses Gesetz, im Originalwortlaut heißt es „Gesetz über die Nutzung und Sicherung von Archivgut des Bundes", gilt seit 2 Jahren. Es ist verdienstvoll, dass der Nomos Verlag mit dem vorgelegten Werk eine Lücke geschlossen hat. Verdienstvoll ist auch, dass diese Leistung von namhaften Experten auf dem Gebiet des Archiv- , Medien- und Informationszugangsrechts (Christoph J. Partsch als Herausgeber sowie Axel Mütze, Norman Koschmieder und Sven Berger) erbracht wurde. Wenn vereinzelt Kritik daran geäußert wird, dass kein Archivar mitgewirkt habe, so schmälert das nicht die Qualität der juristischen Darstellung, wenngleich zuzugeben ist, dass die Sichtweise des im Archiv Tätigen in der einen oder anderen Frage eine interessante Bereicherung dargestellt hätte.

Die Handkommentare des Nomos Verlages sind im wesentlichen Praktikerkommentare. So ist es auch hier: Der Kommentar zum Bundesarchivgesetz wird sich gut eignen für die Arbeit in der Praxis. Die gesetzlichen Erläuterungen sind durchweg verständlich geschrieben, so dass auch Nichtjuristen in der Lage sein werden, sich schnell einzulesen und Orientierung zu finden. Abgesehen vom Abdruck der Archivgesetze und Archivbenutzungsordnungen aller Bundesländer findet sich in dem Band ferner das Sicherheitsüberprüfungsgesetz, ein Benutzungsantrag für das Bundesarchiv und anderes. Besonders zu erwähnen ist der Gesetzentwurf zum Bundesarchivgesetz mit Begründung (Bundestags-Drucksache 18/9631). Die vollständige Aufnahme der Erwägungen des Gesetzgebers in den Band ist eine gute Idee, die man sich bei anderen Kommentaren auch wünschen würde. Sie erleichtert die Arbeit.

Besonders interessant ist die Einleitung zum Kommentar des Bundesgesetzes, welche 50 Seiten im Oktavformat umfasst. Es wird gut herausgearbeitet, dass „historische Forschung ohne Archive nicht möglich ist". Die Funktion des Archivs geht nach Partschs zutreffender Auffassung darüber hinaus, da es sich beim Archiv auch um eine „Stätte der demokratischen Vergewisserung eines Rechtsstaats" handele und der Zugang zu Archiven ein Menschenrecht darstelle.

Die Kritik am nach herrschender Meinung zutreffenden normgeprägten Zugangsanspruch zu Archivalien, formuliert unter Verweis auf das unhistorische Verständnis von Informationsfreiheit in der deutschen Geschichte, überzeugt nicht. Eine wesentliche Handlungsform des Rechtsstaates sind generell-abstrakte Gesetze, auf deren Grundlage das Handeln der öffentlichen Gewalt bestimmt wird. Außerdem wurde die erwähnte „seit 1804 in den U.S.A. bekannte Informationsfreiheit" erst im Jahr 1967 zu einem gesetzlichen Anspruch im Freedom of Information Act.

Insgesamt ist der historische Abriss lesenswert; auch die Übersicht über div. Informationszugangsgesetze (Verbraucherinformationsgesetz, Umweltinformationsgesetz, Geodatenzugangsgesetz, u.a.) ist gelungen. Ein Gleiches gilt für den Überblick über internationale Entwicklungen.

Die Darstellung datenschutzrechtlicher Aspekte der Archivierung von amtlichen Unterlagen bedarf einer breiteren Diskussion. Bekanntlich steht der Zugang zu Archiven und zu amtlichen Informationen zum Datenschutz in einem Spannungsverhältnis, das in einer differenzierteren Betrachtung ausbuchstabiert werden sollte. Zukünftige Rechtsprechung und Rechtsanwendung werden den Weg weisen. Die nicht belegte Behauptung des Herausgebers, dass „der Zugang zu Archivgut bis heute durch den Datenschutz stark und überbordend eingeschränkt" werde, kann die Diskussion eröffnen. Dass die Schutzfristen des Bundesarchivgesetzes dem „Spannungsverhältnis zwischen Forschungsfreiheit und Datenschutz" in ausreichender Weise Rechnung tragen, ist vertretbar.

Lesenswert ist schließlich die Erwähnung von zeithistorisch und juristisch Wichtigem, wie beispielsweise das in der Mephisto-Entscheidung des Bundesverfassungsgerichts betrachtete postmortale Persönlichkeitsrecht, die Nutzung von Unterlagen der Geheimdienste durch die Öffentlichkeit (NS, NSU) sowie die Reaktion des Gesetzgebers auf Desinformation („fake news") durch das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken und die Bedeutung des Rechts auf Informations- bzw. Archivzugang zwecks Widerlegung von Falschmeldungen.

Dem Kommentar zum Bundesarchivgesetz darf man weitere Auflagen wünschen.



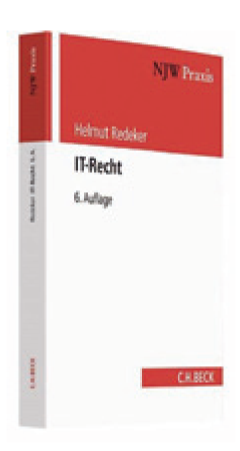
Schläger, Uwe; Thode, Jan-Christoph (Hrsg.)
Handbuch Datenschutz und IT-Sicherheit
2018, 1. Auflage, 662 Seiten,
ISBN 978-3-503-17727-1, 94,- €

(wh) Dieses Buch soll Recht und IT systematisch verbinden und ein Buch sein, das juristische und IT-sicherheitsrelevante Fragen erstmals konsequent verknüpft. Mit Dr. Uwe Schläger, der nicht nur einer der beiden Herausgeber ist, sondern auch den „Teil G: Rechtliche Grundlagen der Informationssicherheit" und Abschnitte von „Teil I: Technische und organisatorische Maßnahmen" zu verantworten hat, ist ein Datenschützer an Bord, der insbesondere im Bereich des technischen Datenschutzes über umfassende, langjährige Erfahrungen verfügt.

Der „Teil A: Datenschutzrechtliche Grundlagen" gibt mit 90 Seiten einen kompakten aber gleichwohl umfassenden Überblick über die Entwicklung des Datenschutzes und das aktuelle Datenschutzrecht in Deutschland, Europa und anderswo. Die folgenden Teile B bis F arbeiten die in Unternehmen relevanten Datenschutzthemen ab. Da geht es von Datenschutzmanagement über die Verarbeitung von Beschäftigtendaten sowie Kundendaten weiter zur Datenverarbeitung im Inter- und Intranet zur Videoüberwachung. Diese ca. 380 Seiten sind thematisch gut strukturiert und gehen auf die in Betrieben und Unternehmen häufig anzutreffenden Fragestellungen mit praktischen Lösungsansätzen ein. Best-Practise-Beispiele und Ausblicke auf künftige Entwicklungen runden einzelne Abschnitte ab.

Die Teile G bis J legen dagegen den Schwerpunkt auf die Informationssicherheit. Neben der EU-Datenschutz-Grundverordnung (DSGVO) wird bei der Darstellung der Rechtsgrundlagen zur IT-Sicherheit auf das IT-Sicherheitsgesetz sowie auf einschlägige bereichsspezifische Gesetze, wie z.B. das Kreditwesengesetz eingegangen. Dem Informationssicherheitsmanagement ist ein – wenn mit 20 Seiten auch nur knapper – eigener Teil des Werkes gewidmet, der allerdings irritierenderweise mit dem Titel „IT-Sicherheitsmanagement" überschrieben ist. Der mit 76 Seiten etwas umfangreichere „Teil I: Technische und organisatorische Maßnahmen" lässt erwarten, dass hier nun die vom Verlag versprochene „konsequente Verknüpfung" von juristischen und IT-sicherheitsrelevanten Fragestellungen zu finden ist. Leider wird diese Erwartung enttäuscht. So fehlt zum Beispiel im Abschnitt „Behandlung von Sicherheitsvorfällen" jeglicher Hinweis darauf, dass ein IT-Sicherheitsvorfall dann, wenn personenbezogene Daten betroffen sind, auch meist eine Datenschutzverletzung darstellt, ebenso wie ein Verweis auf den Abschnitt „5: Meldepflicht bei Datenpannen" im „Teil B: Datenschutzmanagement" und umgekehrt. Trotz dieser nur losen und nicht unbedingt systematischen Verbindung der sich mit dem Datenschutzrecht beschäftigenden Teile A bis F auf der einen Seite und der die Informationssicherheit behandelnden Teile G bis J auf der anderen Seite stellt dieses Werk ein gutes und nützliches Hilfsmittel

sowohl für Datenschutzbeauftragte wie für IT-Sicherheits- bzw. Informationssicherheitsbeauftragte dar.



Redeker, Helmut:
IT-Recht
2017, 6. Auflage, 515 Seiten,
ISBN 978-3-406-68727-3, 79,- €

(wh) Zielgruppe dieses Werkes sind laut Verlag „Rechtsanwälte, insbesondere Fachanwälte für IT-Recht, Richter sowie Syndikusanwälte in der IT-Branche".

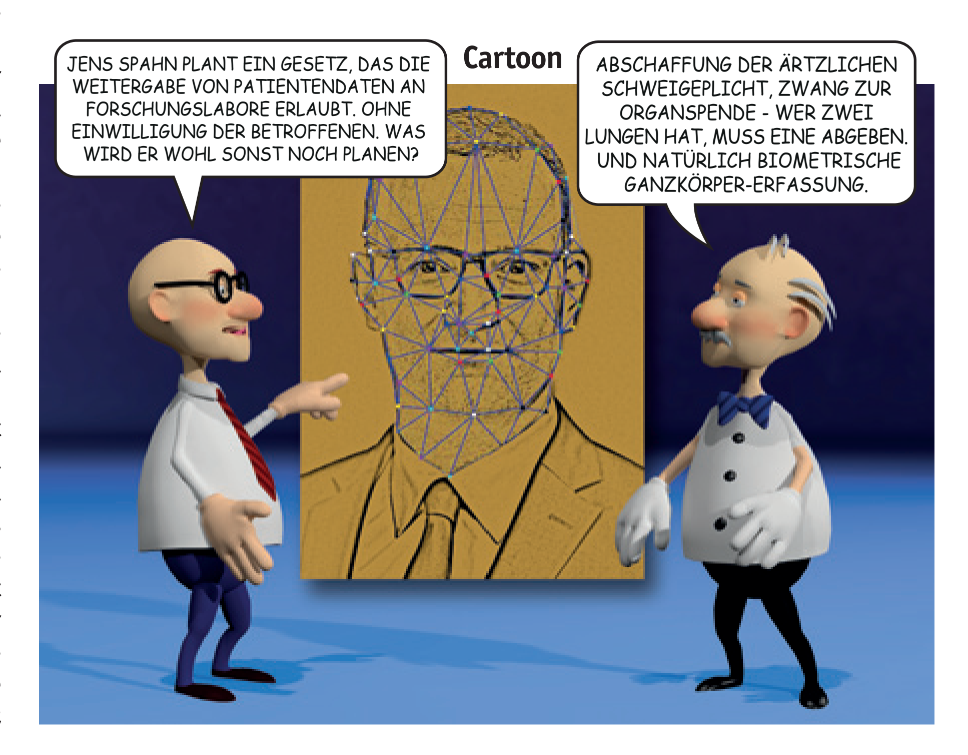
Dass sich nur ca. 4 Seiten mit den Änderungen durch die EU-Datenschutz-Grundverordnung (DSGVO) beschäftigen, ist sicher der Tatsache geschuldet, dass dieses Werk in der aktuellen Auflage bereits Anfang 2017 erschienen ist und die Überarbeitung laut Vorwort „im Wesentlichen im Juni 2016 abgeschlossen wurde", also nur anderthalb Monate nach der Veröffentlichung der DSGVO im Amtsblatt der EU. Hier ist zu erwarten, dass die Änderungen, die sich durch die DSGVO ergeben haben, in einer eventuellen künftigen Neuauflage in den einzelnen Abschnitten, die sich mit dem Datenschutz beschäftigen, eingearbeitet werden.

Suchen nun die am Datenschutz interessierten Leserinnen und Leser im Inhaltsverzeichnis nach ebendiesem, dann findet sich nur ein Abschnitt „9) Datenschutzanforderungen" im Unterkapitel „II. Die Übermittlung von Willenserklärungen im Internet" des Kapitels „D. Rechtsprobleme von Internet und Telekommunikation". Erwähnt wird, dass in datenschutzrechtlicher Sicht für Internet- und Telekommunikationsdienstleistungen in erster Linie das (alte) Bundesdatenschutzgesetz (BDSG-alt), sowie die datenschutzrechtlichen Normen des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) relevant sind. Direkt danach findet sich der Hinweis, „Für vertiefende Auseinandersetzungen sei auf die umfangreiche Speziallliteratur verwiesen". Dieser Verweis ist in der Tat wichtig und richtig, da der darauffolgende Satz „All diese Normen werden Anfang 2018 durch [die] dann geltende europäische Datenschutzgrundverordnung (DSGVO)" ersetzt." irritiert. Eine etwas konkretere Zeitangabe, wie z.B. 25. Mai 2018 statt „Anfang 2018" wäre hier ebenso wünschenswert gewesen, wie zumindest die Wörter „Ein Teil dieser Normen" anstelle von „All diese Normen".

Irritierend ist auch, dass in diesem Abschnitt „Datenschutzanforderungen!", der sich ja im Unterkapitel „II. Die Übermittlung von Willenserklärungen im Internet" befindet, ganz allgemein die datenschutzrechtlichen Anforderungen im Zusammenhang mit der Erbringung von Internet- und Telekommunikationsdienstleistungen erörtert werden, die datenschutzrechtlichen Anforderungen an eine Einwilligung dagegen nur auf etwa anderthalb der insgesamt 22 Seiten dieses Abschnittes dargestellt werden. Inhaltlich hätte es dieser Abschnitt – nach entsprechender Aktualisierung bezüglich der DSGVO – verdient ein eigenes Unterkapitel in Kapitel D zu sein. Dann hätte auch der Anhang direkt als letzter Abschnitt dieses Unterkapitels seinen passenden Platz gehabt. In diesem findet sich dann überraschender Weise die im Großen und Ganzen weitgehend richtige Aussage: „Die datenschutzrechtlichen Sonderregelungen des TMG entfallen, nicht jedoch die des TKG, das auf der E-Privacy-Richtlinie beruht (Art. 95 DSGVO)." (besser wäre die Formulierung gewesen, „die auf der E-Privacy-Richtlinie beruhen", da ja nicht das ganze TKG der Umsetzung der E-Privacy-Richtlinie dient.

Im Stichwortverzeichnis finden sich dann noch weitere Stellen, die sich mit dem Datenschutz beschäftigen, so zum Beispiel ein Abschnitt „Datenschutz: insbesondere Auftragsverarbeitung" als Nebenpflicht zu einem Rechenzentrumsvertrag.

Der vom Verlag benannten Zielgruppe kann summa summarum empfohlen werden, dem Verweis des Autors auf die Spezialliteratur zum Thema Datenschutz zu folgen. Für Datenschützerinnen und Datenschützer, die sich auch mit Gebieten des IT-Rechts (wie rechtlicher Schutz von Software, rechtliche Aspekte bei Beschaffung von Hard- und Software oder Produkthaftung) beschäftigen müssen, stellt dieses Werk eine nützliche Übersicht dar.



CHINESISCHE GERICHTE

verteilen Bonuspunkte

- wenn man sich vorbildlich um ältere Familienmitglieder kümmert
- wenn man Hilfsbereitschaft bei Nachbarn zeigt
- wenn man die Taten der Regierung in den sozialen Medien lobt
- wenn man Geld für wohltätige Zwecke spendet
- wenn man gesunde Babynahrung kauft
- wenn man sich ehrenamtlich engagiert
- wenn man ein chinesisches Auto fährt
- wenn man Blut spendet
- wenn man eine gute finanzielle Lage vorweisen kann
- wenn man regelmäßig regierungstreue Webseiten besucht
- wenn man Biogemüse kauft

strafen durch Herabstufung des Scorewertes

- wenn man Freunde mit einem schlechten Scorewert hat
- wenn man die Stromrechnung nicht pünktlich bezahlt
- wenn man ein Taxi bestellt und nicht erscheint
- wenn man sich zu lange mit Online-Videospielen vergnügt
- wenn man sich weigert, Militärdienst zu leisten
- wenn man im Internet Pornos anschaut
- wenn man bei der Internetsuche die falschen Fragen stellt
- wenn man über das Regierungssystem lästert
- wenn man bei rot über die Ampel läuft
- wenn man sich an der Ladenkasse vorgedrängelt hat
- wenn man bei Onlinekäufen Waren oft zurückschickt
- wenn man an Demonstrationen teilnimmt

Ab 2020 wird in China das verpflichete Bewertungssystem für alle eingeführt. China mit seiner Totalüberwachung ist weit weg? Firmen wie Payback mit dem Bonuspunktesystem und Krankenkassen mit kostenlosen Fitnessarmbändern wissen, wie es vielen Menschen in Deutschland mit der Aussicht auf Belohnungen schmackhaft gemacht werden kann.